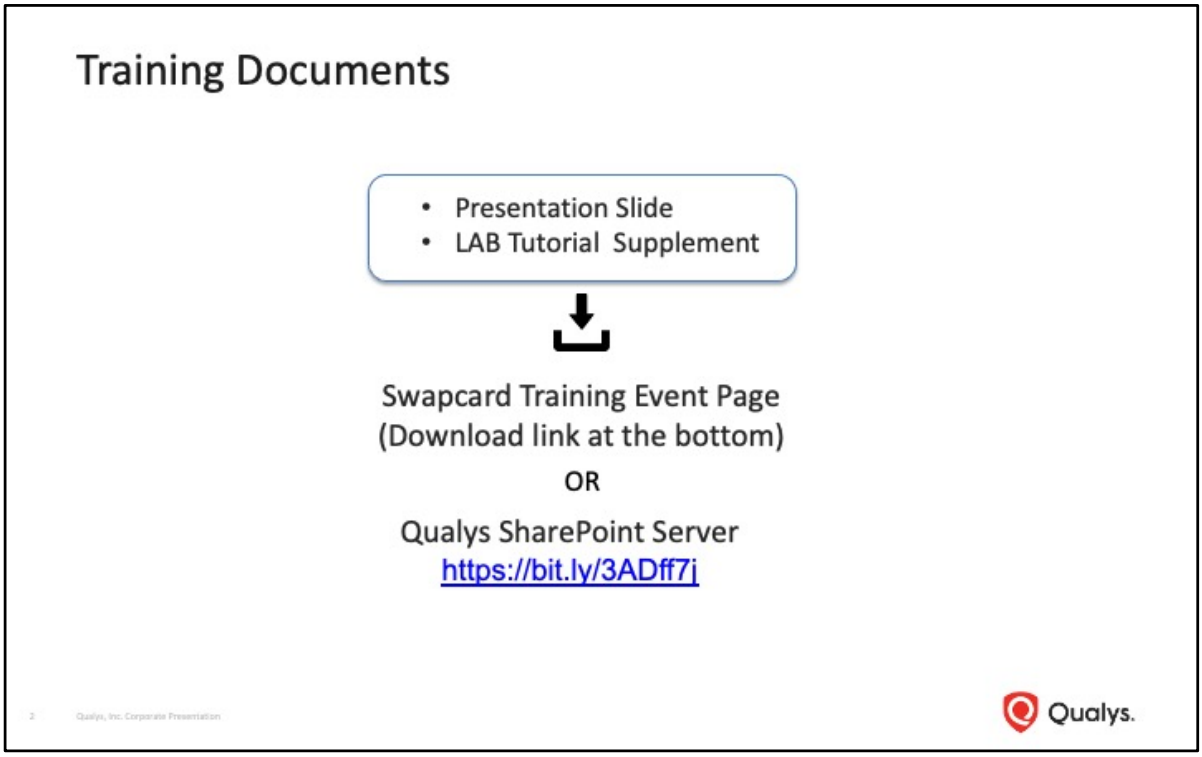
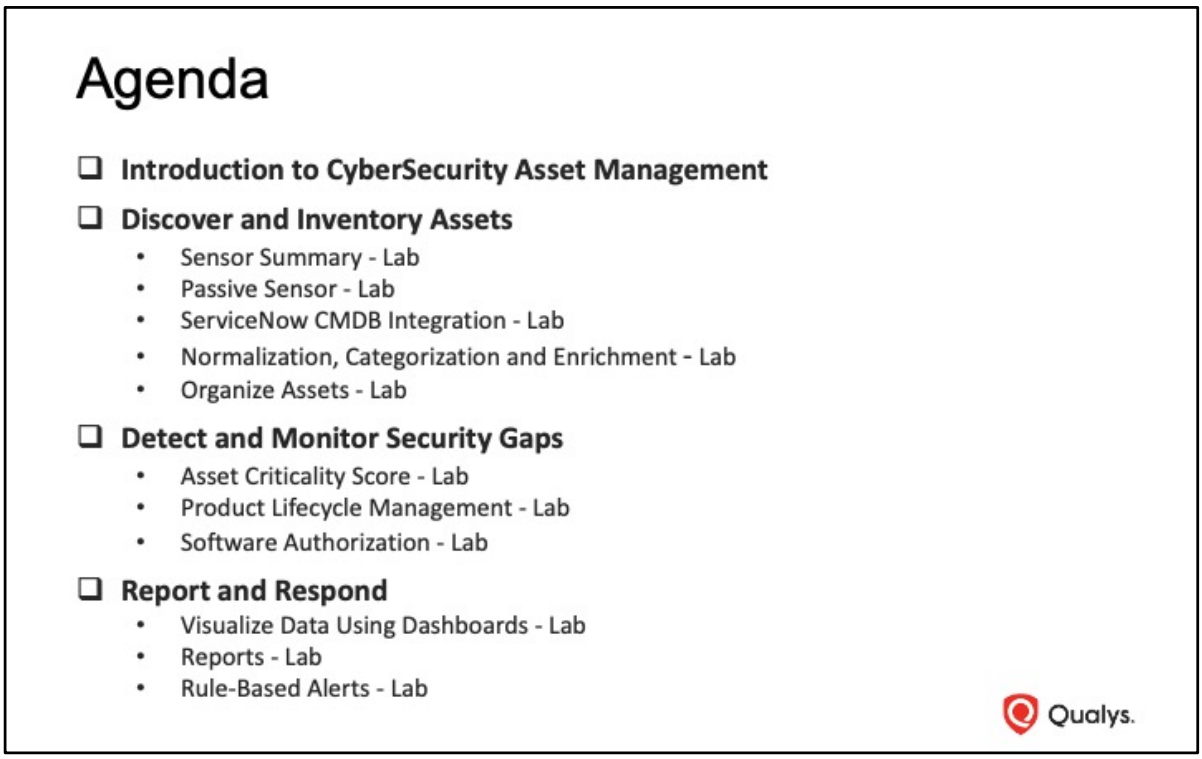
Welcome to this training on Qualys CyberSecurity Asset Management. In this course you will learn about the Qualys CyberSecurity Asset Management application and apply its use cases to discover, organize, prioritize and manage your asset inventory.



You will need to download the training documents needed to complete the CyberSecurity Asset Management course from the Qualys learning portal qualys.com/learning.

Note that you will need a PDF reader like Adobe Acrobat to view these files.



This is the agenda for the class today. The overall message of this course is to discuss how to view all your assets in one place, and how to organize, manage, prioritize and refer to those assets to provide a clear process for your organization when it comes to scanning, reporting, querying, and dashboarding.

We will begin the course with an overview of Global AssetView (GAV) and CyberSecurity Asset Management (CSAM) and the use cases supported by these applications.

We will then understand the different Qualys Sensors that are used to collect data from your IT environment to support asset inventory, Vulnerability Management, Policy Compliance and other Qualys applications.

Extending on the Sensors topic, we will discuss the use case and configuration for the Passive Sensor.

Moving further, we will understand how CSAM enriches Qualys inventory with business information derived from ServiceNow CMDB integration.

Thereafter we will understand how Global AV and CSAM perform normalization, categorization and data enrichment of the asset inventory data to provide vital context needed to understand your IT infrastructure.

Then we will look at setting up Asset Tags to better organize and manage assets for scanning and reporting tasks.

Next, we will discuss how you can focus your security prioritization efforts on high-importance and high-risk assets, by defining the Asset Criticality Score.

Next, we will discuss the product lifecycle management feature in CSAM that provides visibility into End-of-life / End-of-Sale and End-of-Support dates for hardware and software products.

Moving forward, we will discuss how to define and create lists of both Authorized and Unauthorized software and track the result in your IT environment.

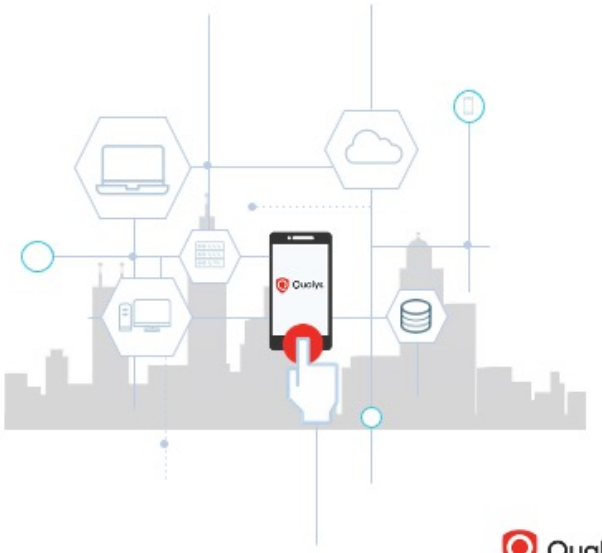
Next, we will discuss how to visualize asset data using dashboards and configure reports to satisfy company and regulatory needs.

Lastly, we will conclude the training with a discussion on configuring rule-based alerts to automatically notify interested parties of at-risk assets.

This section provides an overview of CyberSecurity Asset Management solution and its use cases.

Modern IT Environments are Hybrid

Cloud
On-premise
Workstations
Mobile workforce
OT/IIoT/IoT

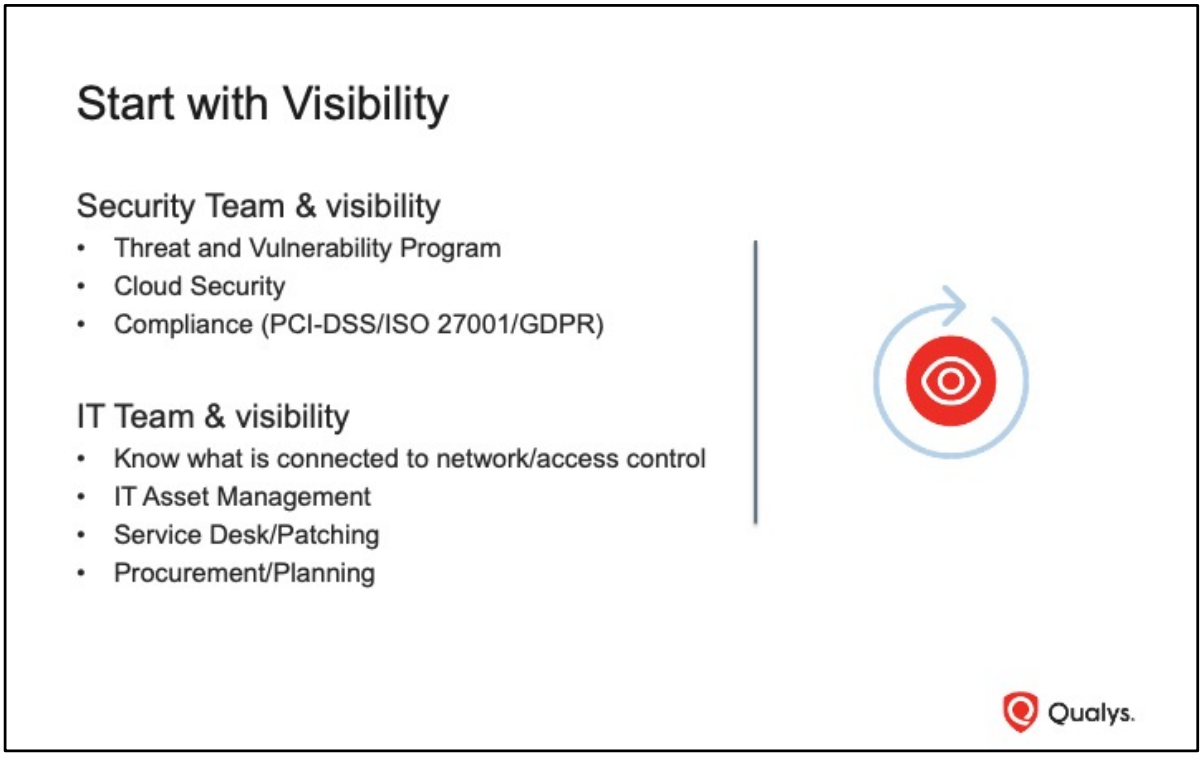


Qualys.

We are going to start with the problem modern IT teams have.

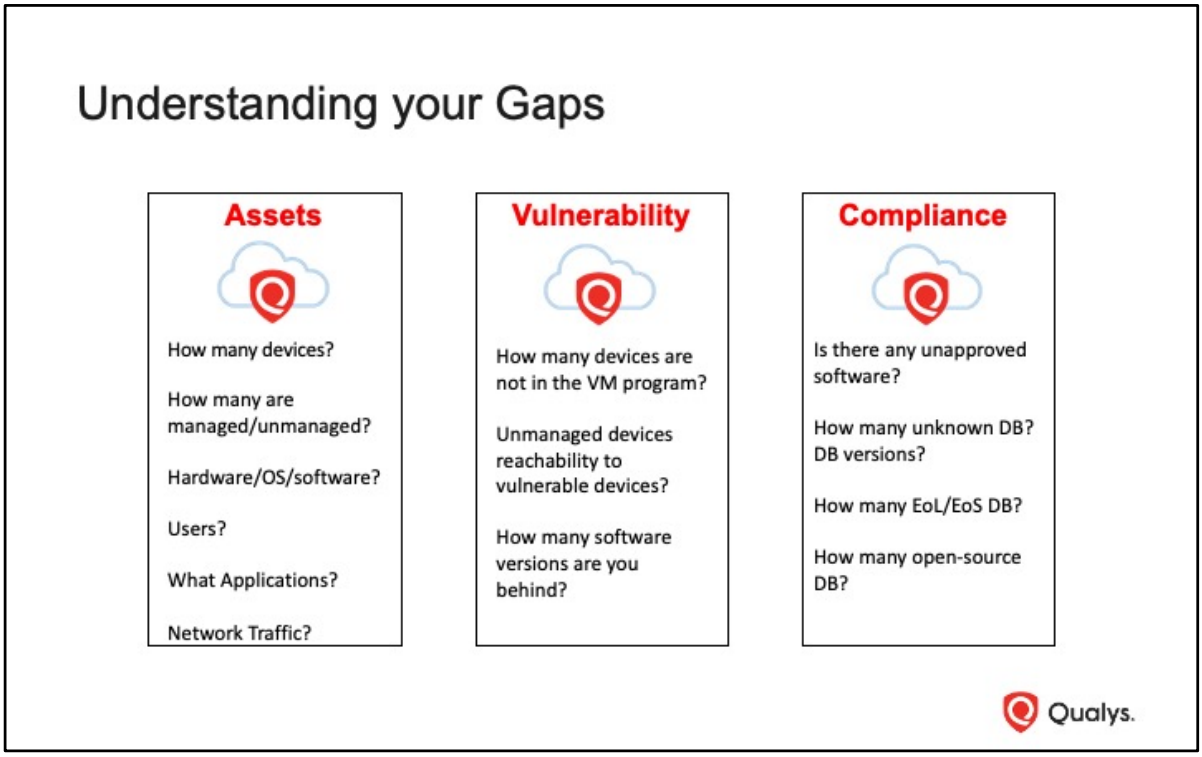
You cannot secure, what you do not know. The problem is that visibility today is much more complicated than visibility even 20 years ago. You used to be able to run a network mapping tool, find everything in your network, and then start securing it.

Today, you have so many more (and different) environments to manage. You may have a Cloud environment. Does the security team manage that? Or is it IT? Or maybe you have a Cloud team. Then you have on-premise workstations. That's IT. You might also have a mobile workforce and Operations technology (OT), Internet of things, Industrial internet of things (IIoT), etc.. How can you see those assets and secure them?



Security Team
Security is going to start with visibility. If you are trying to gauge the threat to your organization, you first must know your attack surface.
For cloud security you will also need to know about your assets deployed in cloud architectures. If they are ephemeral, compliance becomes extra important.
If you are running a vulnerability program, knowing your assets helps you understand what needs to be patched and where is there unnecessary software and hardware deployed that increases the risk to the organization.
For compliance, you need to know which assets are compliant and which ones aren't. That starts with knowing what is deployed in various places throughout the organization.

IT Team
If you are going to have any sort of network access control, you'll need to know what is connected to your network. How close are unmanaged assets to your vulnerable assets?
Patching requires visibility. You can't patch something if you don't know about it.
Visibility is also required for planning. By having an understanding of what's deployed in your network, you'll be able to see how technology needs to evolve.

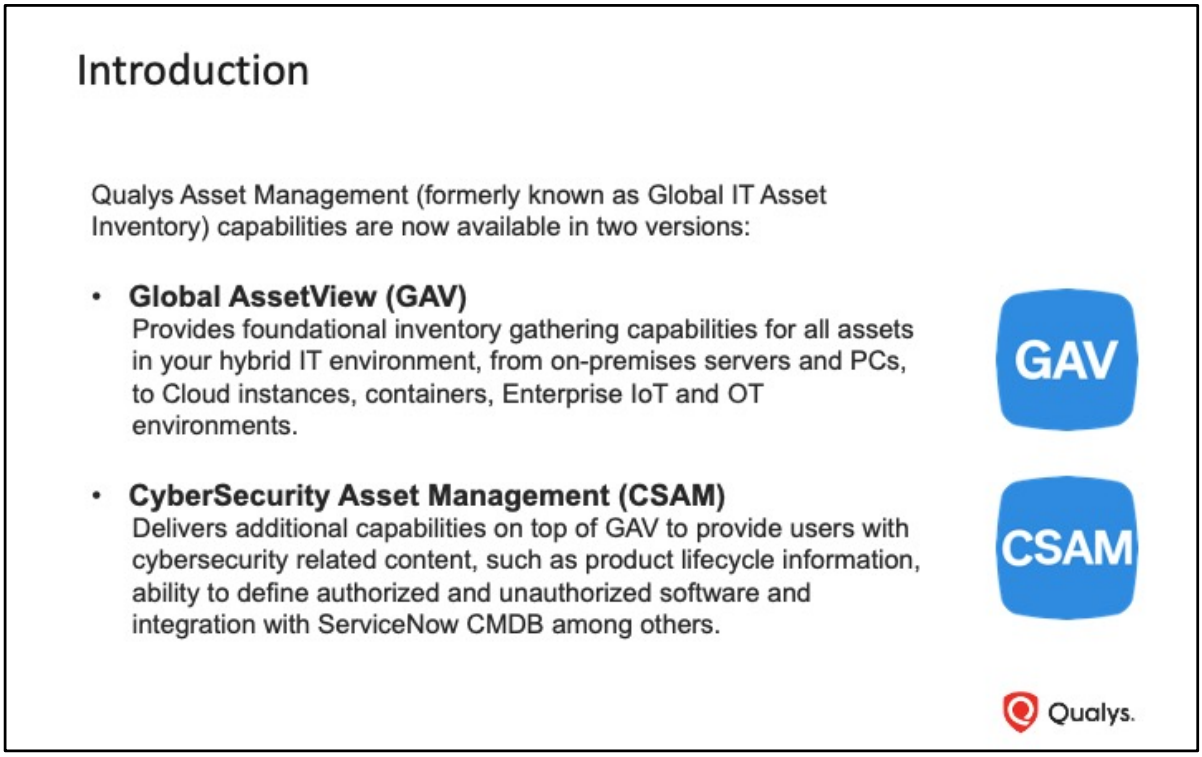


Understanding gaps in a network is as difficult as ever.

First, you start with Assets. Simply having an inventory. How many devices are in your network? How hard is it to get a picture of your managed and unmanaged devices? If you are able to get a number of those assets, what do you know about those assets (context) ? What type of hardware and software do you have deployed? What kind of network traffic flow do you have?

After you know about your devices, which ones are you actively scanning? Or do you have a Cloud Agent deployed? How close are those unmanaged devices to your vulnerable devices? Do you have vulnerable software deployed or out of date software?

Are you controlling approved software at all? How much of your software is end of life or end of support?



Qualys CyberSecurity Asset Management (formerly known as Global IT Asset Inventory) capabilities are available in two versions:

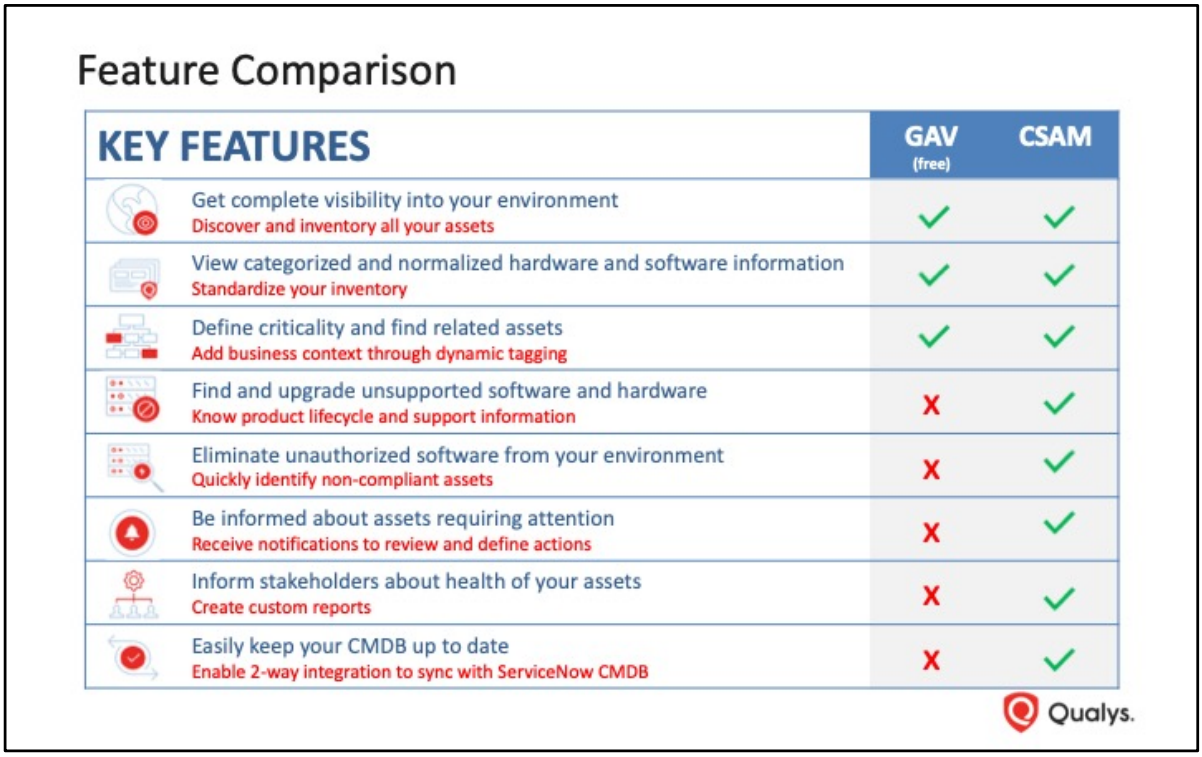
- Global AssetView (GAV)
- CyberSecurity Asset Management (CSAM)

GAV (which is free) lets you:

- Obtain asset inventory across hybrid environments
- View normalized and categorized hardware and software inventory information
- Add custom tagging to automatically organize your assets and rank their criticality
- Create and view customizable dashboards and widgets
- Search any asset in seconds

On top of GAV, upgrading to CSAM will also include:

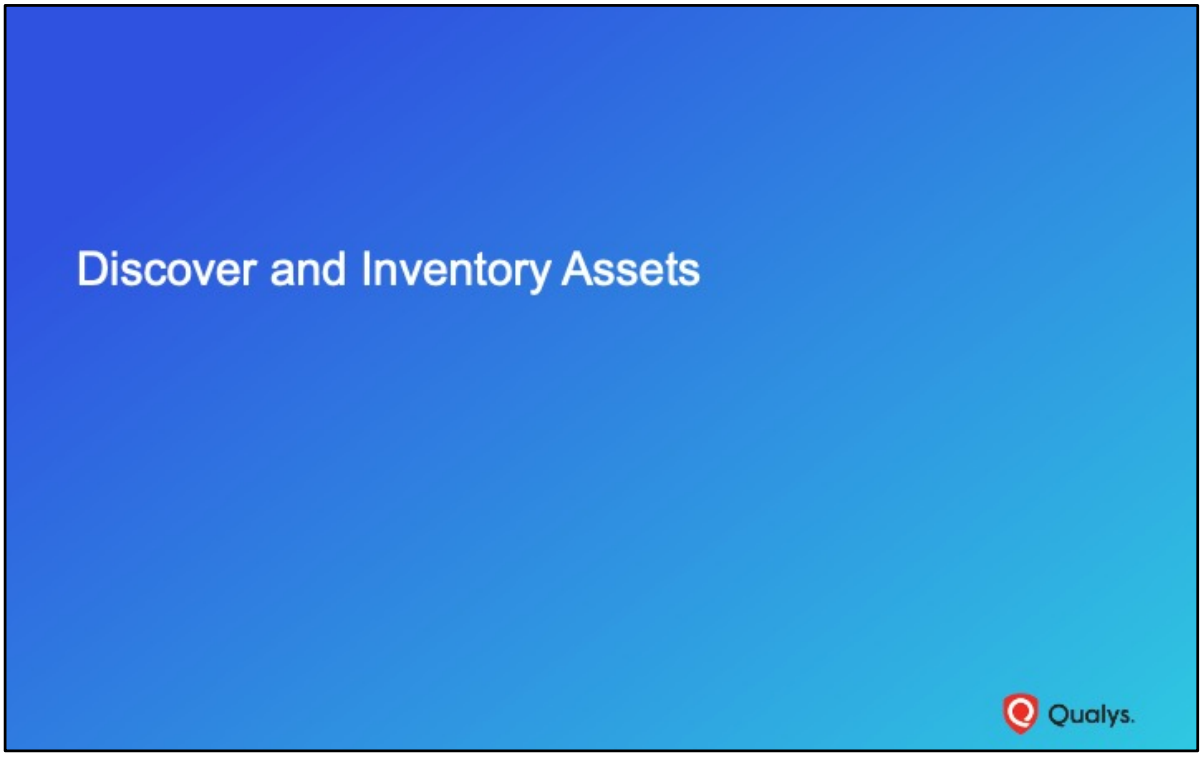
- Enriched asset data – hardware & software lifecycles, licenses categories, and more
- Bi-directional synchronization of asset data with your ServiceNow CMDB
- Ability to define and manage authorized and unauthorized software in your organization
- Customizable reporting to meet internal and external needs (e.g. standards compliance reporting)
- Alerting via email, Slack or PagerDuty to inform you about assets requiring attention



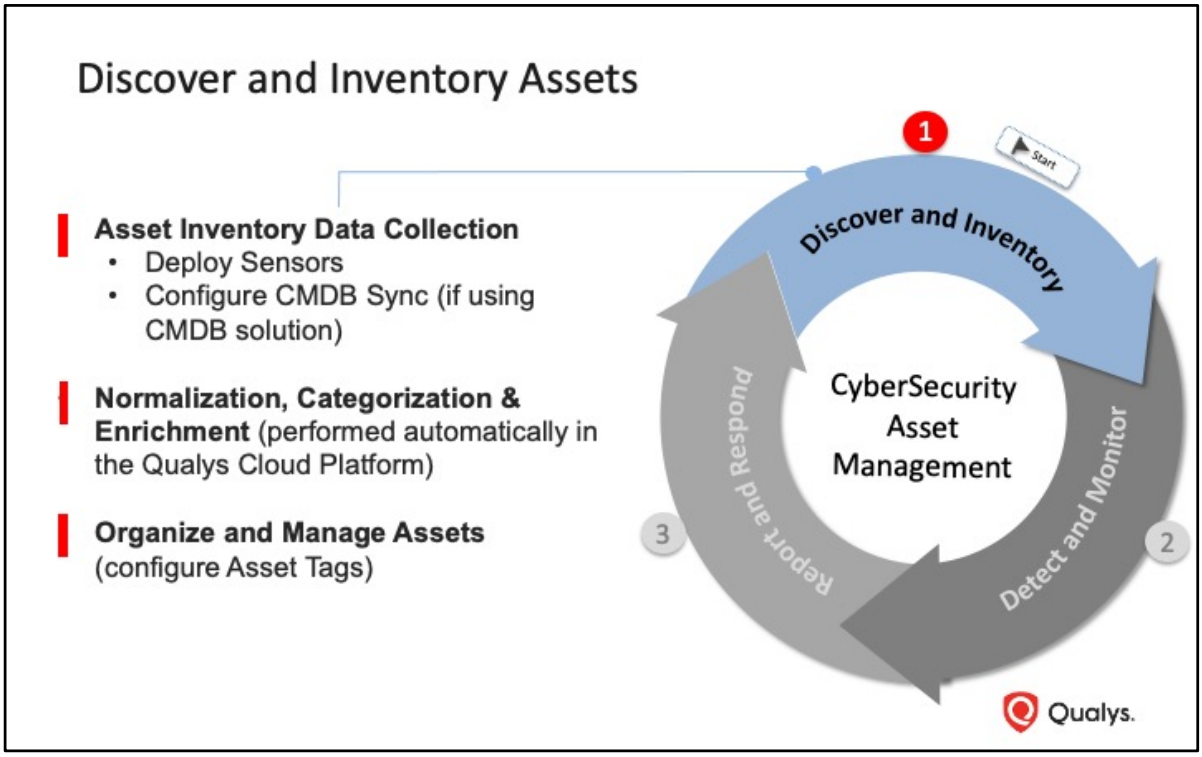
The table in the slide provides a high-level feature comparison between Global AssetView (GAV) and CyberSecurity Asset Management (CSAM).

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 detection of security gaps and CMDB integration, plus alerting and response.



This section provides an overview of the various Qualys sensors that collect data from your hybrid IT environment.



The functionality available in CyberSecurity Asset Management (CSAM) can be divided into three (3) sets of capabilities:

- Discover and Inventory
- Detect and Monitor
- Report and Respond

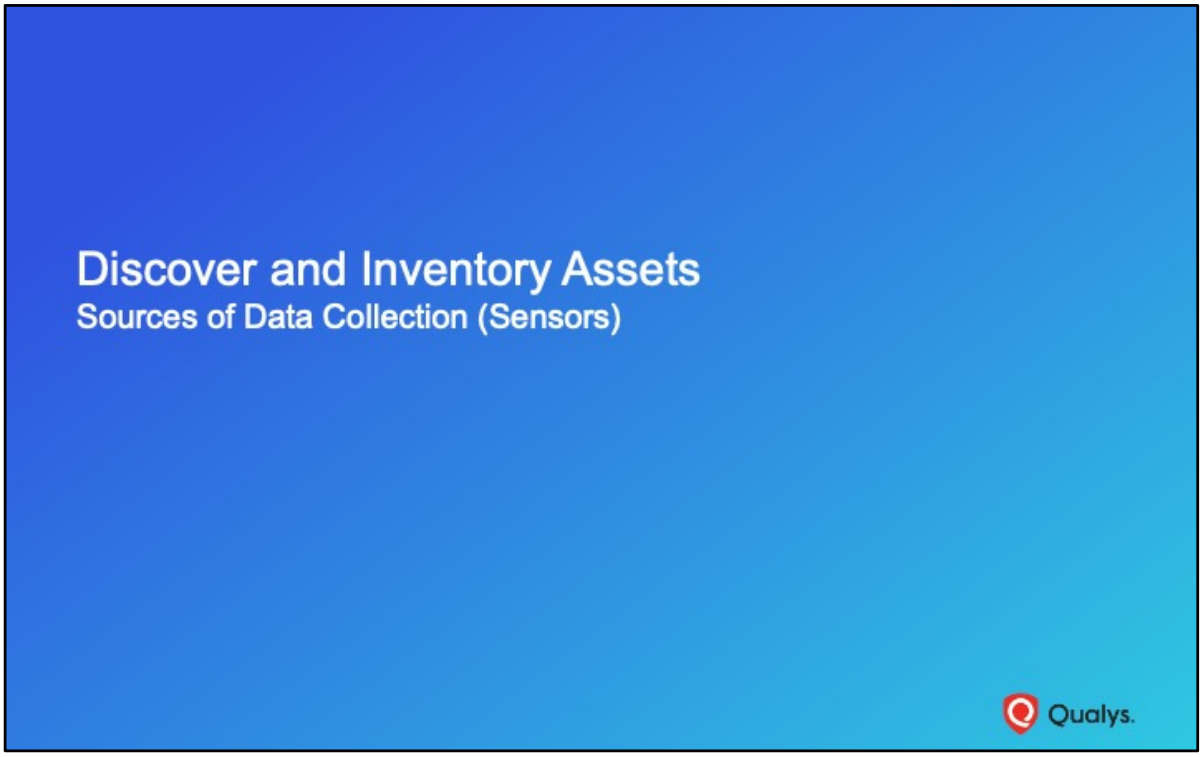
Discover and Inventory

Qualys Asset Management, begins (step 1) by identifying and managing assets throughout your enterprise architecture. Qualys has various sensor types that collect data for you.

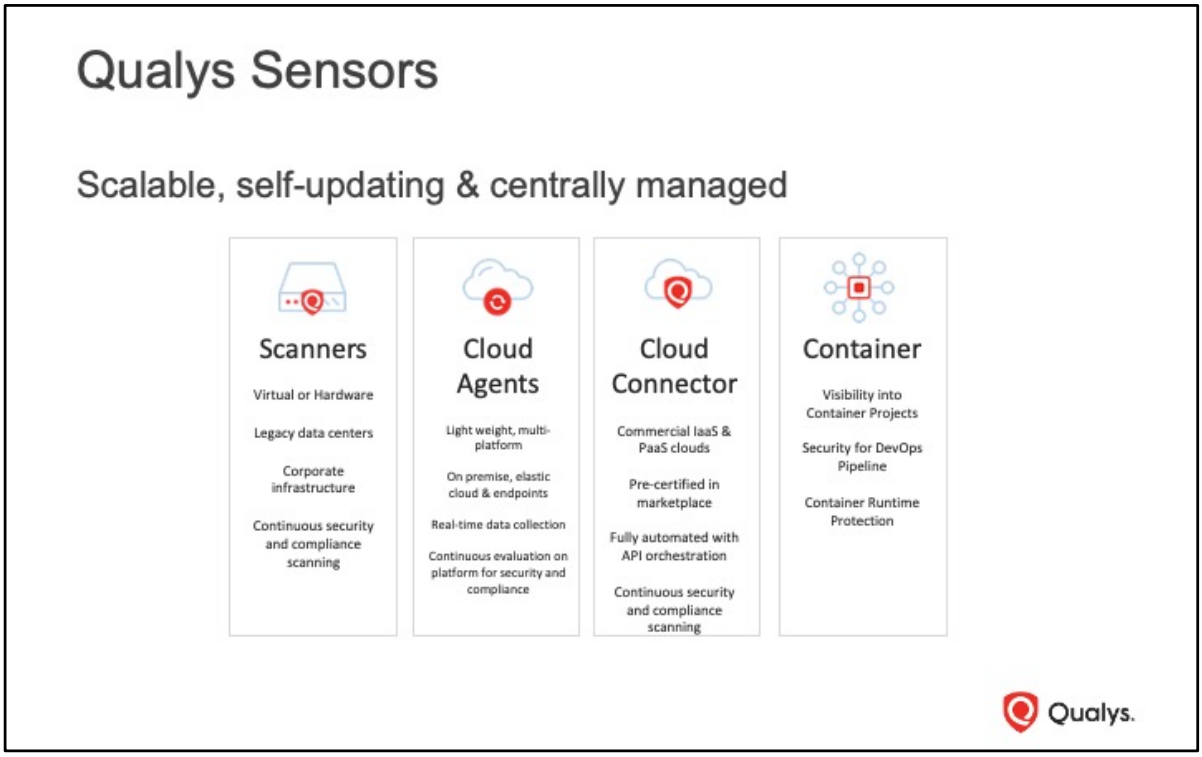
Qualys Global AssetView (GAV) / CyberSecurity Asset Management (CSAM) work with hybrid sensors to continuously discover and dynamically monitor all IT Assets, across your hybrid environment. GAV/ CSAM use the data provided by these sensors and then normalize and categorize it into standardized names and structures.

And you can also enrich asset inventory with business context from CMDB sync.

Asset Tags help you to organize and manage assets.

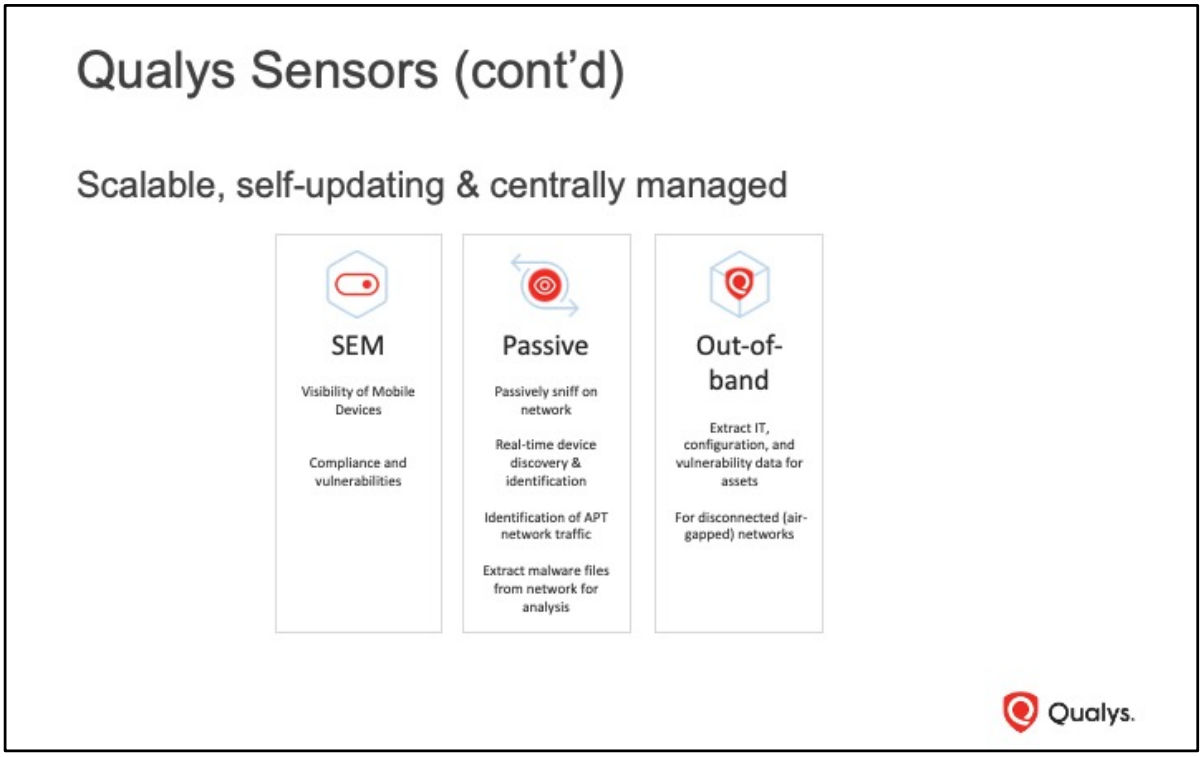


This section provides an overview of the various Qualys sensors that collect data from your hybrid IT environment.

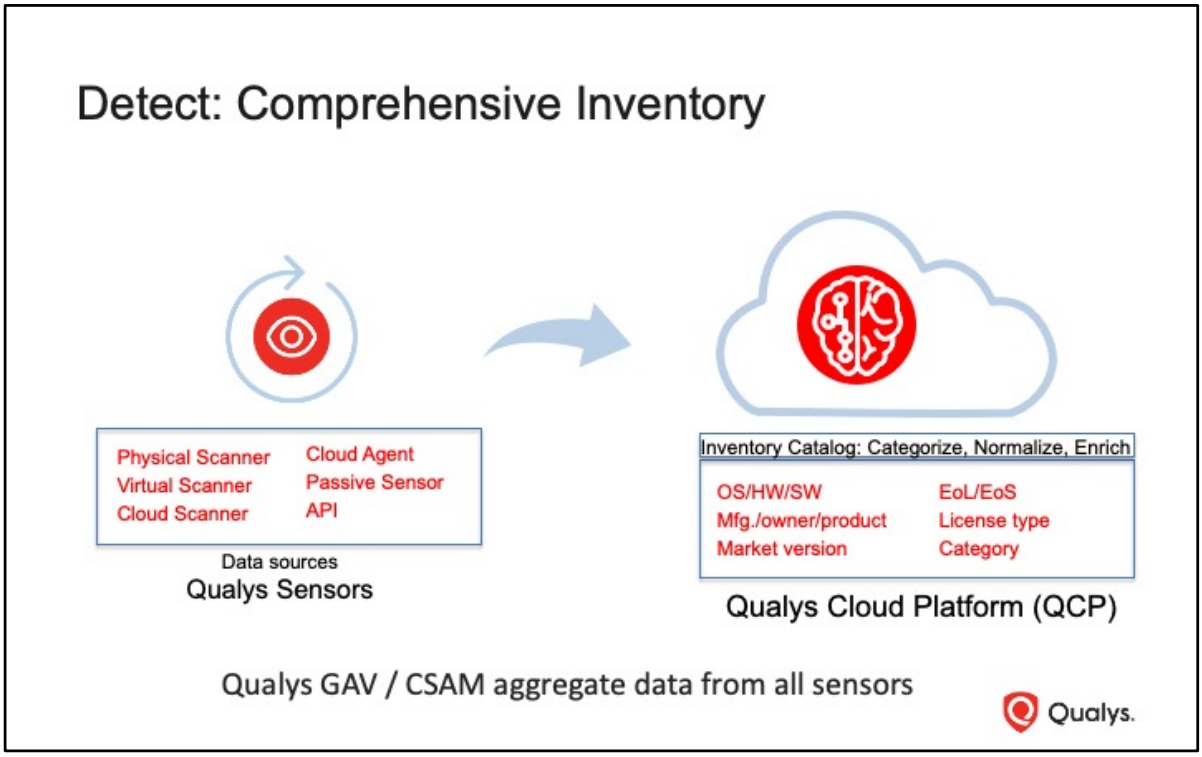


Qualys has various sensor types that collect data for you.

Scanner Appliances: External (on the internet) and internal scanners, physical or virtual, used to scan on-prem or cloud assets. Qualys has a training class on scanning.
Cloud Agent: lightweight agents that can be installed on clients and servers for real-time visibility. Ideal for assets with dynamic IP, remote/roaming users, ephemeral cloud instances, and systems sensitive to external scanning. Qualys has a training class on Cloud Agent.
Cloud Connectors: collect metadata from cloud platforms such as Amazon Web Services, Microsoft Azure and Google Cloud Platform. Qualys has a training class on Cloud Security which covers Cloud Connectors.
Container Sensor: Available as an image for Docker-based containers, designed to discover, track and continuously secure containers – from build to runtime. Qualys has a training class on Container Security. Qualys has a training class on Container Security.



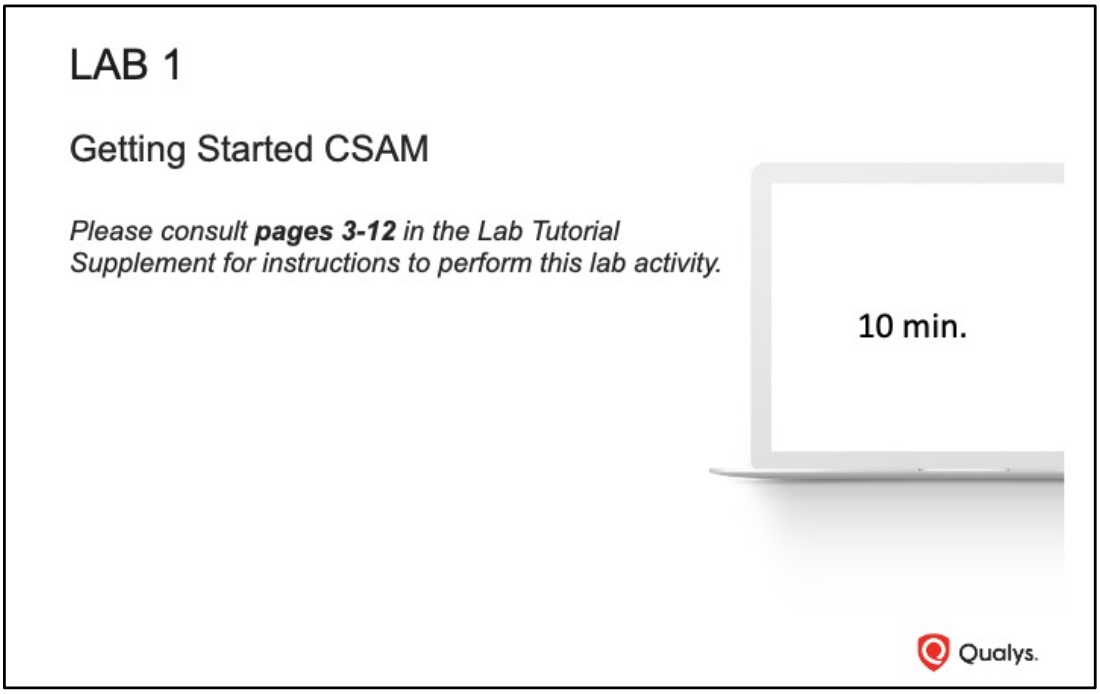
Secure Enterprise Mobility – Apps/agentless deployed on mobile assets. You get visibility can verify rooted phones, passcode missing and other configuration settings.
Passive Sensor: Available as physical or virtual appliance, continuously monitors all network traffic, profiles devices and flags any asset activity.
Out-of-band Sensor: Out-of-band configuration assessment helps you extract IT, configuration, and vulnerability data for assets deployed on disconnected (air-gapped) networks.



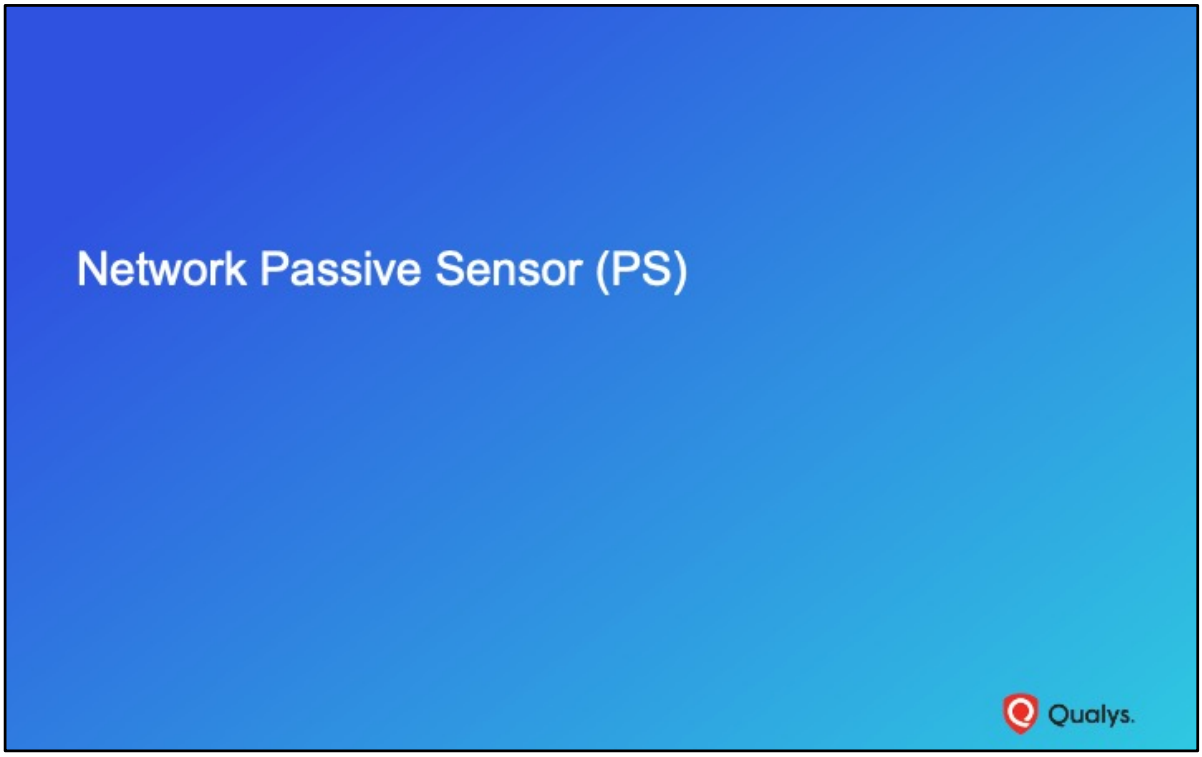
The Qualys Sensors are all populating the the platform with your inventory, vulnerability, threat, compliance, cloud, and web app data. This gives you your data in one place.

Whenever you are going to build a report, query data, or build a dashboard, you are using data that has populated into the platform from your sensors.

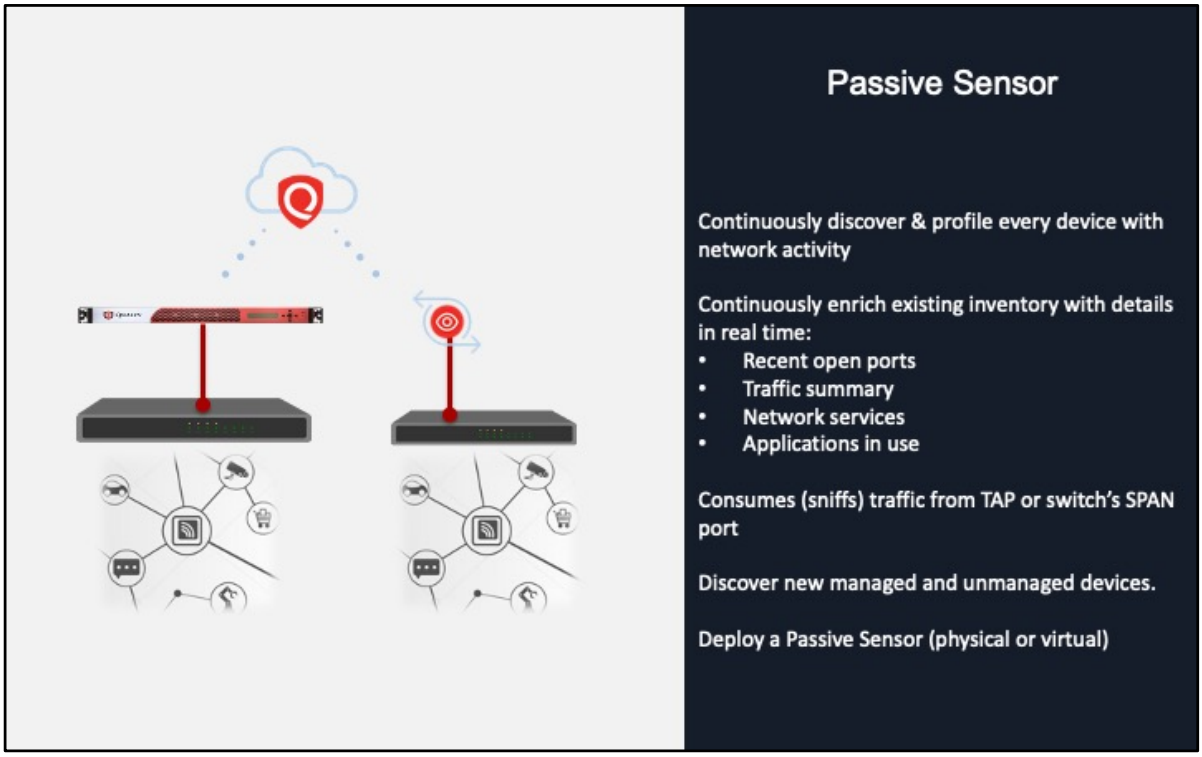
GAV / CSAM aggregate and correlate the data gathered by all Qualys sensors giving you a comprehensive, detailed inventory of all your hardware and software, as well as a multi-dimensional view of your global, hybrid IT environment.



Lab 1 will provide an overview of CSAM and help you understand how to search and filter asset data in the Inventory section in the CSAM user interface.



This section provides an introduction to the Passive Sensor.



Passive sensor helps you eliminate blind spots in your network where you don't know what is connecting to your infrastructure.

Qualys Passive Sensor connects to the SPAN port of a switch deployed at layer-2 (e.g. distribution layer) for best results. Essentially, it is a traffic sniffer that monitors the mirrored traffic from the switch in real-time.
It discovers assets the moment they connect to the network and start communicating. It extracts metadata from the network traffic to identify assets, their attributes and the traffic flows. It then posts this meta data periodically to the Qualys Cloud Platform.

Note: Passive Sensor does not send full traffic packets to the Cloud, unless specified sample is initiated by the user for troubleshooting purposes.

New assets are reported within 5-10 minutes. As more information is discovered it is aggregated across all assets and sent every 30 minutes. Asset information is then visible through Qualys CSAM.

- New assets (not seen before in the Subscription) are flagged as unmanaged assets.
- Existing managed assets (e.g. already scanned or with cloud agent) are enriched.

Additionally, and when the subscription is enabled for traffic analysis, summarized traffic information is sent to the Qualys Cloud Platform every 30 minutes for traffic

analysis use cases.

Passive Sensor comes in a virtual and hardware appliance.

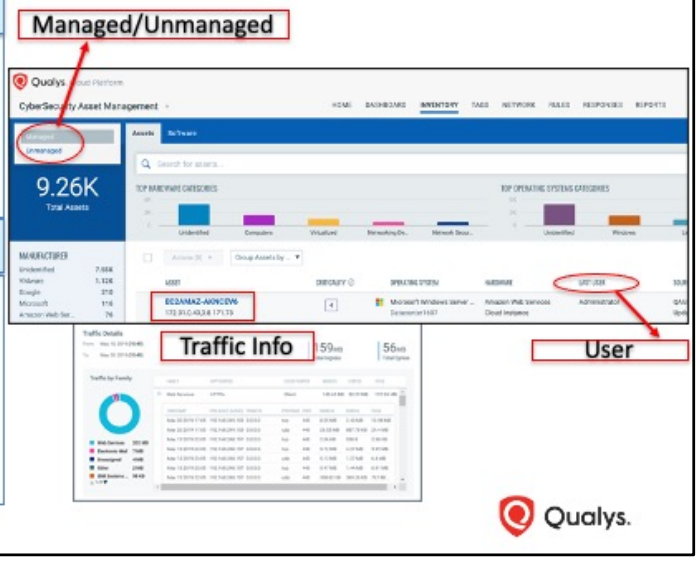
Discovery Example: Unmanaged Devices

Problem

- Identify unmanaged devices that are not managed by IT security
- Know what resources are being accessed by these unmanaged devices
- Know who is using these devices

Asset Inventory Capabilities

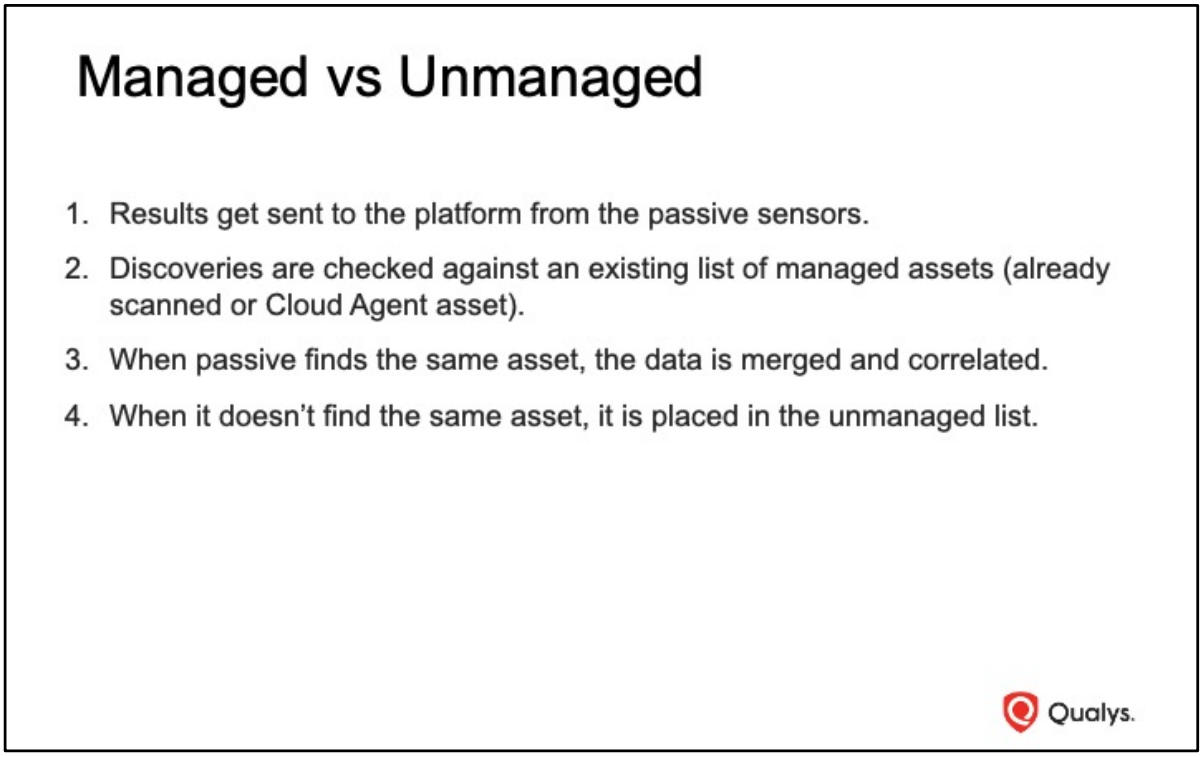
- Discover Managed and Unmanaged devices with detailed context info
- View how these devices communicate with internal assets and external networks
- See what users are using these devices



Before we get into the first major use case of unmanaged devices, let's first talk about managed devices.

Managed devices are those where you've already deployed a Qualys Cloud Agent or have scanned with a Qualys Scanner Appliance. You *know* about those assets. Data about them is indexed in the platform.

But what about those devices that you don't know about. Those that aren't yours, that you aren't managing, and you don't know who using them. Passive sensor will see that user if they connect to your network and have visibility on it. It will understand traffic patterns and open ports.



With the Passive sensor, your data gets sent to the platform based on what is detected.

The first thing that happens is that data for the detected device is checked existing list of managed to assets. If something is being scanned or has an agent, we are going to merge the data we have for the detected host with the data we have for the scanned/agent based host.

If we don't see the asset, you will see the new asset under your unmanaged asset list.

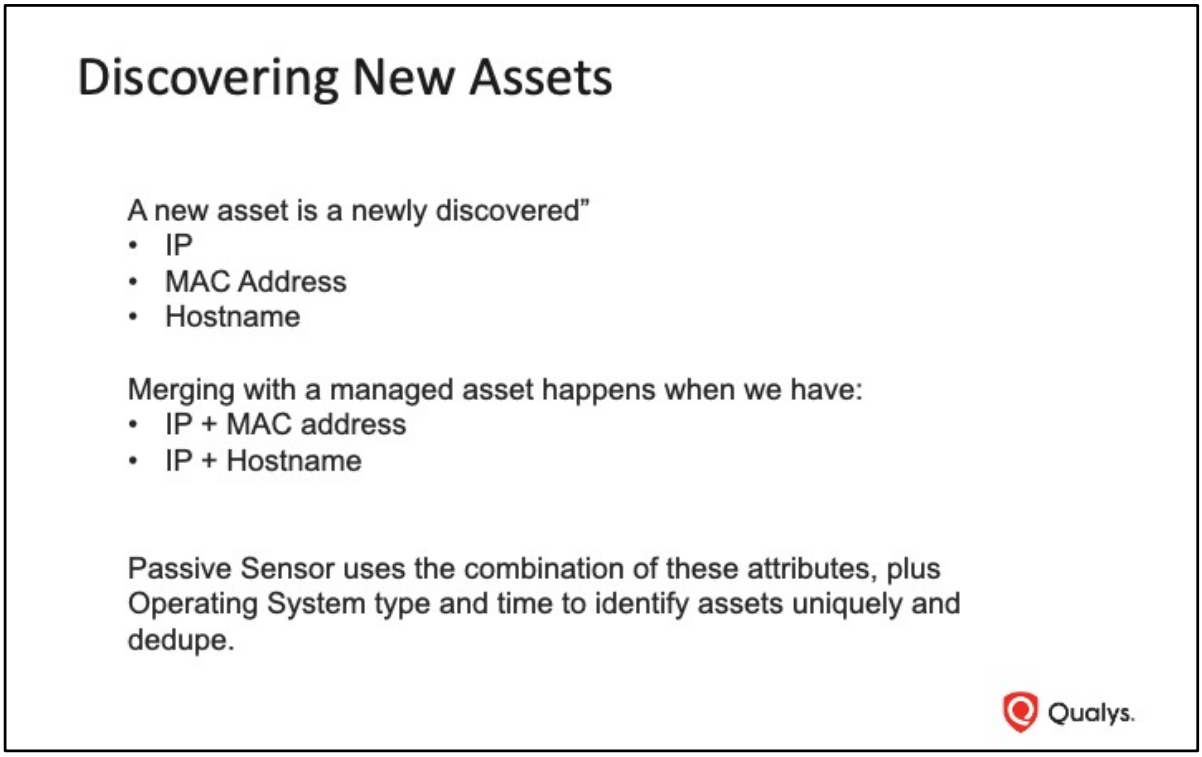
Unmanaged Assets

- It is common to find unidentified or unknown values within the "Unmanaged" assets section of the Asset Inventory application.
- Confidence levels are provided (LOW, MEDIUM, HIGH) for OS and hardware findings.

Qualys.

It's common to find unidentified assets within the "Unmanaged" assets section of the Global AV /CSAM application. For this reason, Qualys adds confidence levels (low, medium, high) to the Operating System and Hardware columns. Remember, you can use the “Quick Actions” menu of any unmanaged asset, to provide feedback to Qualys researchers.

In this illustration, an OS name for the second asset is displayed, but its hardware is “Unidentified.”



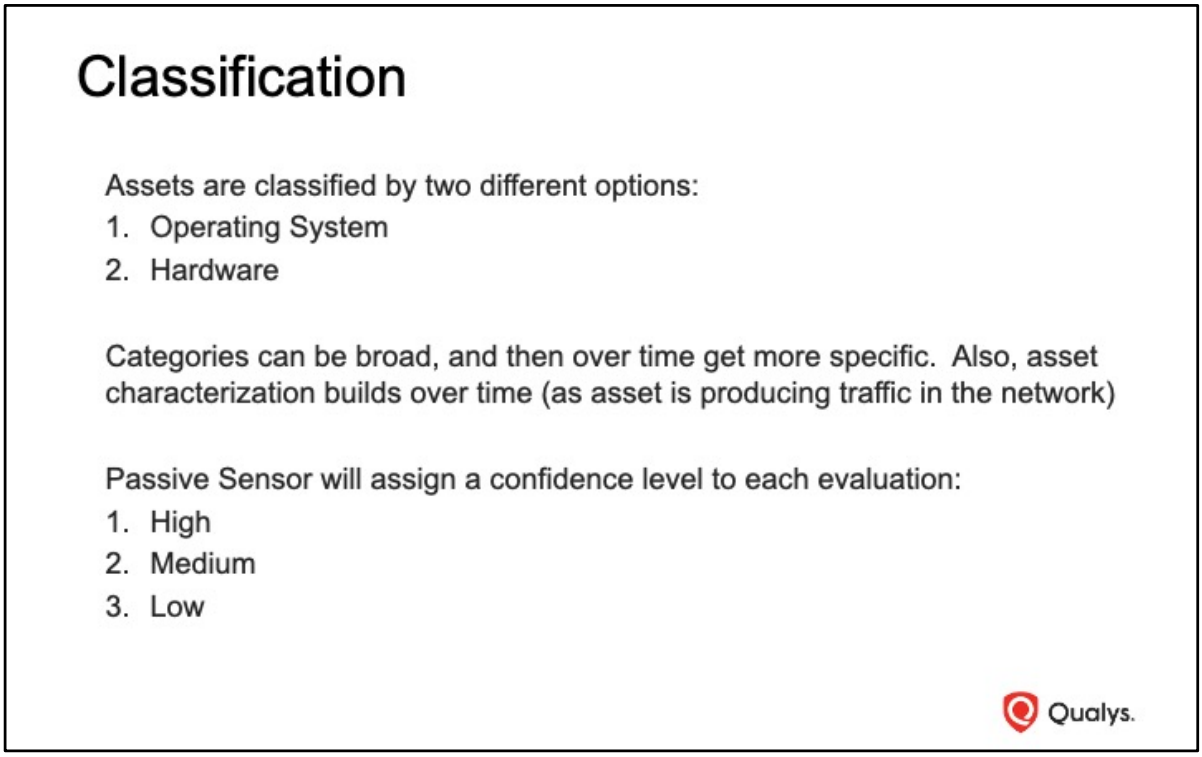
We know the ip address for everything.

At some point we are going to discover the mac address, on the same ip, and we are going to correlate that. On another request, we might see the hostname. Then we can build the profile of the asset. We use a combination plus OS, and type and time and de-dup. same ip, same os type, and we think the same asset.

One asset might have multiple interfaces.

IP + mac, or IP + Hostname will allow us to merge this data with a managed asset.

If we don't see something that matches that, we list it as an unmanaged asset.

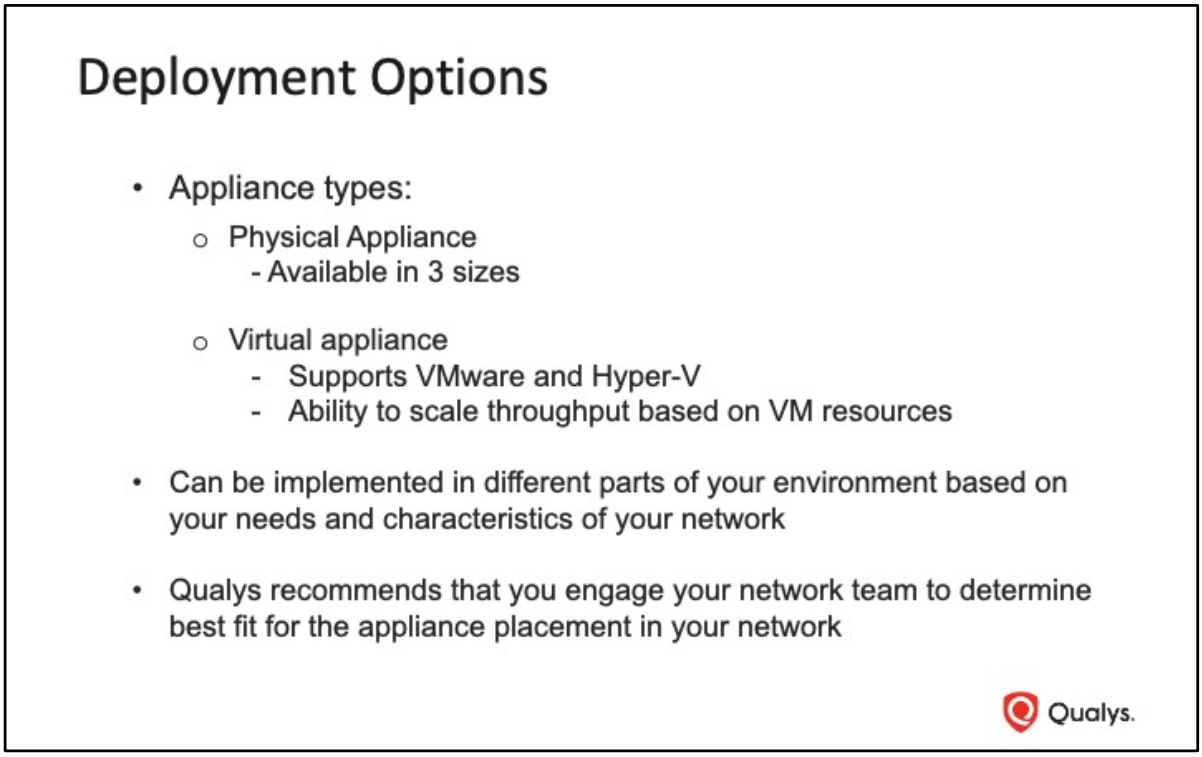


As assets are discovered, Qualys will give an operating system and hardware. Over time, the data we provide for an asset can get more specific.

This classification happens in parallel based on stuff we can see and based on activity of what the devices does on the network.

So why use passive sensor? Unauthenticated scan is something you are getting at one time. You'll see open ports, you'll see Linux, etc.

When you use Passive Sensor, you'll be continually observing traffic. You will see that it's not Linux it's Android, it's Samsung. This is only possible if observing on an ongoing basis.



The Passive Sensor is available as a physical and a virtual appliance.

The physical appliance is available in the following configurations:

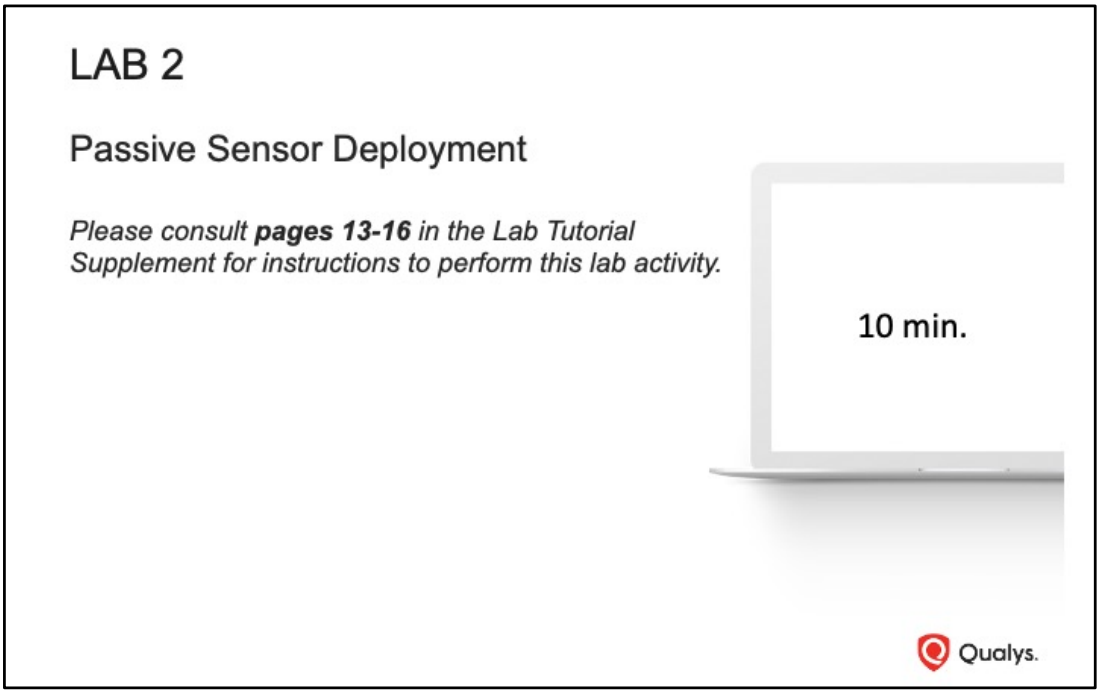
- 1Gbps: Typically, Passive Sensors with Gigabit interfaces would be sufficient for an aggregate traffic not exceeding 900 Mbps for up to 5,000 active assets.
- 4Gbps: Passive Sensors with 10G interface may be required to be attached to discover and profiling up to 10,000 active assets while supporting an aggregate traffic throughput of 4 Gbps per appliance.
- 10Gbps: Passive Sensors with multiple 10G interfaces may be required to be attached to discover and profiling up to 20,000 active assets while supporting an aggregate traffic throughput of 10 Gbps per appliance.

The virtual appliance is available for Microsoft Hyper-V and VMware platforms and offers the flexibility to scale up/down throughput based on virtual machine configuration.

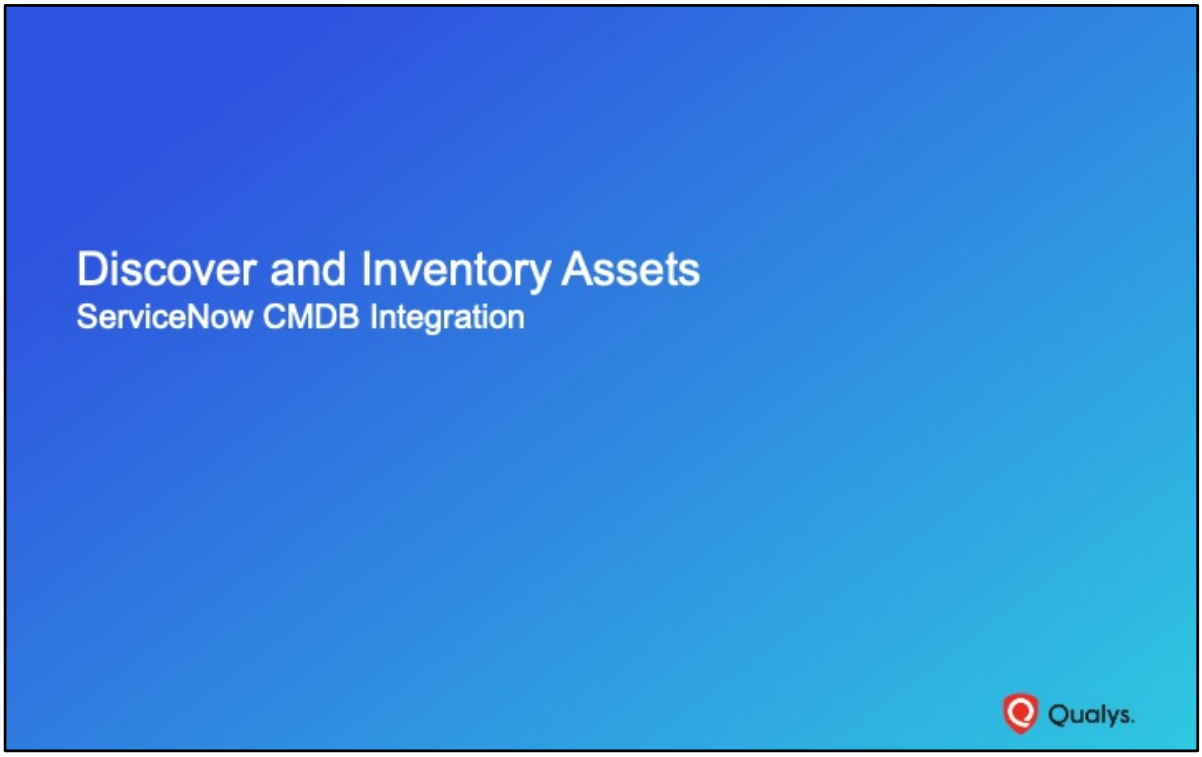
PS appliances can be implemented in different parts of your environment based on your needs and characteristics of your network. It supports mirror traffic using Local SPAN, RSPAN, and ERSPAN method and can be placed at the Distribution layer (better accuracy and visibility) or the Core layer (better coverage).

Qualys recommends that you involve your network team to determine the best fit for the appliance placement in your network.

For more information, refer to the PS Deployment Guide.



Lab 2 will help you understand how to deploy and configure a Passive Sensor in a virtual environment.



This section provides an overview of Qualys integration with ServiceNow CMDB and how it helps security teams to gain comprehensive visibility into your IT asset inventory to immediately flag security and compliance risks.

Certified ServiceNow CMDB Sync App

- Supports 2-way sync (Qualys to ServiceNow and ServiceNow to Qualys)
- Up-to-date, complete, structured, and enriched ServiceNow CMDB
- Enrich Qualys assets with key CMDB business data
- Synchronization schedules can be configured and saved.
- Asset metadata is only synchronized for assets that already exist in both Qualys and ServiceNow.
- Optionally, asset information is staged for user approval before being written to CMDB.
- Preconfigured reports.

Qualys.

ServiceNow (SN) is a third-party application that stores information about all technical services used in an enterprise in a Configuration Management Database or CMDB. Within the CMDB, the support information for each service offering is stored in a Configuration Item (CI) specific to that service. This information includes the service name and description, assignment groups, change management approvers and service roles as well as other information directly related to the service support.

Traditionally, the Qualys API has been used to extract data from the Qualys Cloud Platform; data which is then consumed by your third-party applications. However; with the Qualys ServiceNow CMDB Sync App, metadata can move in both directions.

We can bring in IP addresses of devices not discovered by Qualys, so that we can add them to Active Scanner or deploy Cloud Agent on them and collect inventory - this allows you to ensure that both Qualys and ServiceNow are in sync.

Qualys asset inventory syncs with ServiceNow's CMDB, continuously feeding it fresh data, so the CMDB can accurately map assets' relationships, connections, hierarchies, and dependencies. Supports multiple Qualys accounts / API sources for sync.

Qualys can benefit from metadata in the ServiceNow CMDB and ServiceNow can benefit from Qualys categorization, normalization, and data enrichment.

Asset metadata synchronization is performed only for assets already in both Qualys and ServiceNow (i.e., not for new asset discovery).

Integration with ServiceNow CMDB

Integration Type	ServiceNow Prerequisites	Qualys Prerequisites
Qualys CMDB Sync App	Qualys CMDB Sync App (available in ServiceNow Online Store)	Qualys subscription with CMDB Sync enabled and API access to CSAM module
Qualys CMDB Sync Service Graph Connector App	• Qualys Service Graph Connector App (available in ServiceNow Online Store) • ITOM Visibility license in ServiceNow	Qualys subscription with CMDB Sync enabled and API access to CSAM module

Qualys.

There are 2 Qualys apps for ServiceNow CMDB Sync:

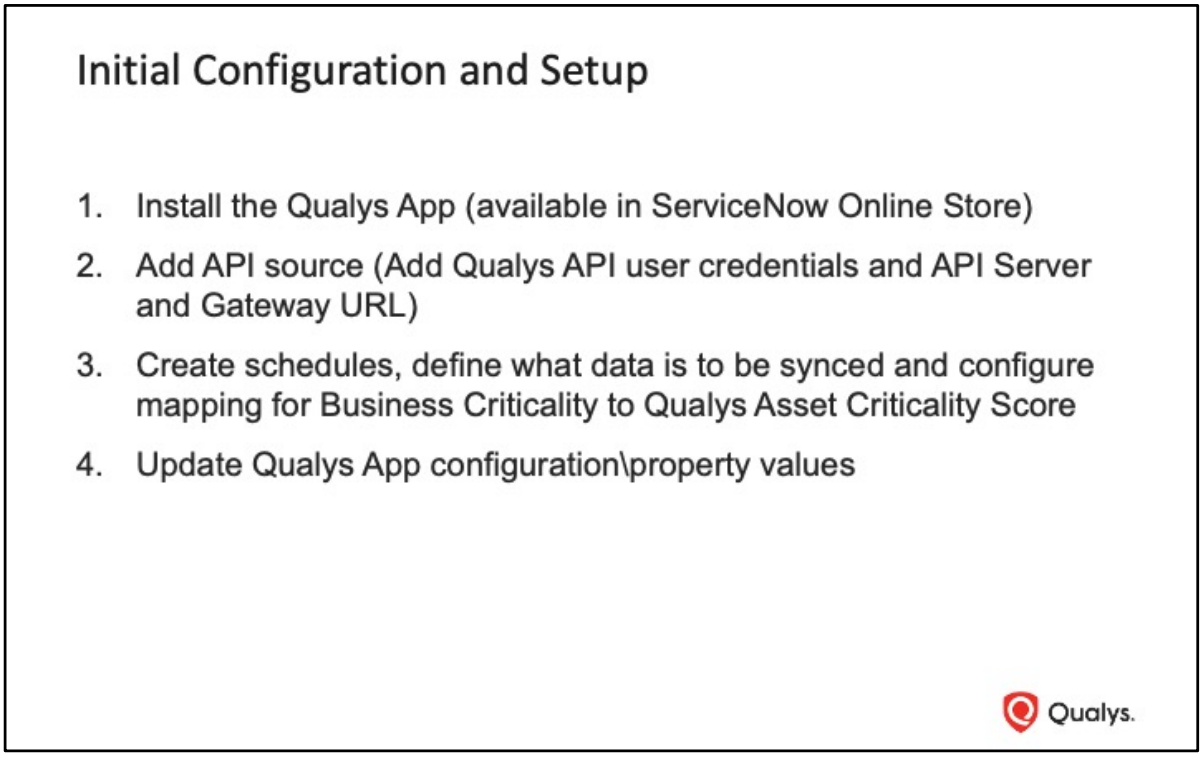
- Qualys ServiceNow CMDB Sync App
- Qualys ServiceNow CMDB Sync Service Graph Connector App

For a detailed description of the Qualys CMDB Sync App, go here: https://www.qualys.com/docs/qualys-cmdb-sync-v2.pdf

The Qualys CMDB Sync Service Graph Connector App is intended for Service Now 'Orlando' and later versions and includes additional features. The Qualys CMDB Sync Service Graph Connector App requires the ITOM Visibility license installed in ServiceNow.

For a detailed description of the Qualys CMDB Sync Service Graph Connector App, go here: https://www.qualys.com/docs/qualys-asset-inventory-cmdb-sync-ire.pdf

For both integration types, you must have a valid Qualys account subscription with API Access to the CSAM module (and Vulnerability Management, if doing VM scan on imported assets).
Also, CMDB Sync must be enabled within your Qualys subscription.



Quick Steps to get started with Qualys ServiceNow CMDB Sync:

1. **Install the Qualys App** - You'll get the app from the ServiceNow Online store. Additional plugins need to be installed in ServiceNow, if using the Qualys ServiceNow Service Graph Connector App. These prerequisite plugin details are listed in the pervious slide.

2. **Add API Source** - Provide the Qualys API Source details. The Qualys API URL you should use for Server and Asset Inventory Server fields depends on the Qualys platform where your account is located. For more information on Qualys platform URLs, see https://www.qualys.com/platform-identification/. After adding the API source, use 'Test Connection' to know if the connection between ServiceNow and the defined Qualys source is working fine.

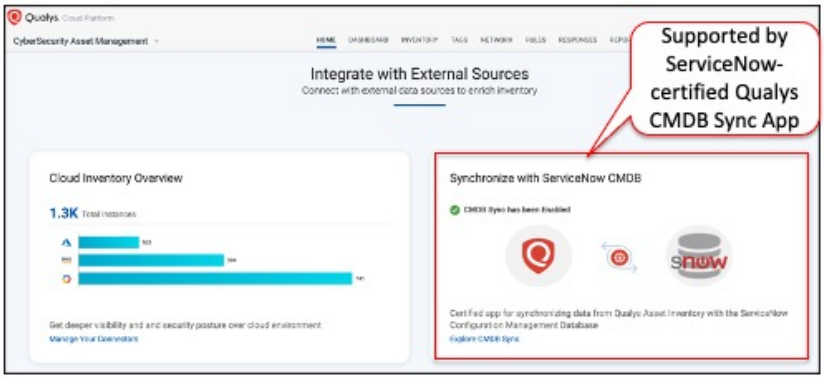
3. **Create Schedules** - Provide details within the Qualys app to create a schedule. You need to set up at least one schedule. You may eventually want many more. Once a schedule is successfully created, the sync between the source and CMDB gets working as per the defined schedule.
   - Asset information is automatically enriched with additional context such as lifecycle date and support stage, license category
   - For assets that already exist in both, asset metadata can be synchronized
   - Optionally, asset information is staged for user approval before being written to CMDB

- Support for multiple Qualys accounts/API sources

1. **Update Properties** - The Qualys app has pre-populated configuration\property values. These values determine the maximum number of assets to be fetched in a single API request call (Qualys to ServiceNow sync), the maximum number of records to be uploaded to Qualys (ServiceNow to Qualys sync), time restrictions on schedule run time and API timeout settings. You can always change these values to suit your needs.

Sync Business Information from ServiceNow CMDB

Automatically import business context attributes from ServiceNow CMDB



Business context helps security teams to:

- Better understand the IT environment
- Apply right scanning strategies
- Prioritize assets and vulnerabilities
- Provide accurate scope to remediation teams

Qualys.

You can also enrich Qualys inventory with business information by importing business context to Qualys, including owners, environment, business applications and other key CMDB data to improve response to asset health issues. This integration is achieved using our ServiceNow-certified CMDB Sync App.

This helps security teams to better understand the environment, organize scans, prioritize assets and vulnerabilities, and provide accurate scope to remediation teams.

Business Attributes Imported into Qualys Asset Inventory

Business Attributes

- Status (e.g., in-repair, lost/stolen)
- Organization (Company, Business Unit, Department)
- Owned By - Who owns the asset
- Managed By - Responsible person
- Supported By – Supporting person
- Environment (e.g., Prod/Lab/Test)
- Assigned Location (Country, City)
- Business App/Service name
- Business Criticality

Accessed using:

- Business Information tab in Asset Details
- Search queries
- APIs

Qualys.

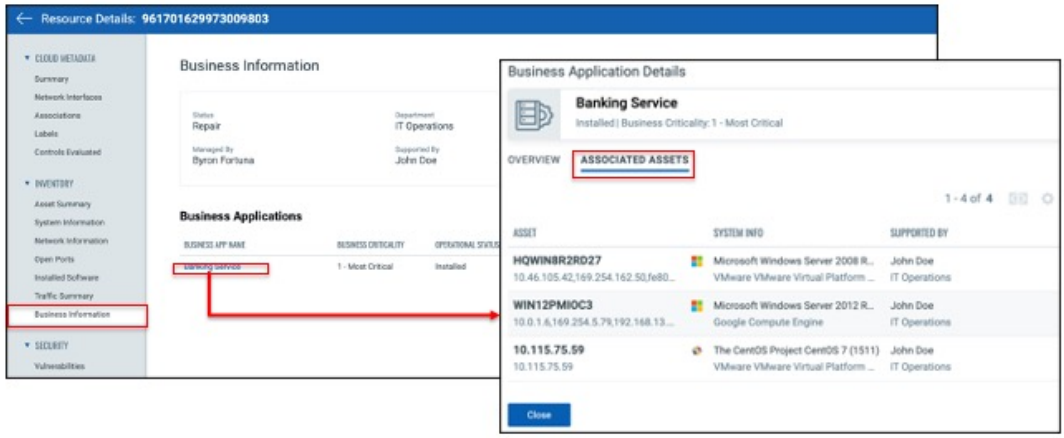
The Qualys CMDB Sync App uses SN APIs. Two new SN APIs are introduced to import some additional metadata of assets and business app to Qualys.

Below is the list of business attributes currently imported in CSAM:

- Status (e.g., in-repair, lost/stolen)
- Organization (Company, Business Unit, Department)
- Owned By - Who owns the asset
- Managed By - Responsible person
- Supported By – Supporting person
- Environment (e.g., Prod/Lab/Test)
- Assigned Location (Country, City)
- Business App/Service name
- Business Criticality

Business information can be seen in Asset details for assets whose inventory data is synchronized with SN CMDB. You can also use search queries to filter assets matching specific business information or use Qualys APIs to export asset data including all business information.

View Business Information in Asset Details



- Derive relevant context on the way the asset is being used, who owns it, what department and business service it belongs to, business criticality, etc.
- See the list of assets associated with a business app

Qualys.

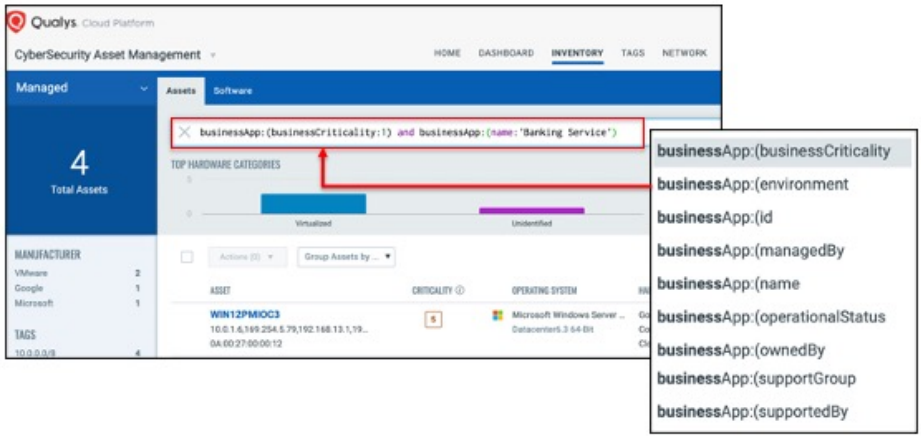
The Business Information and Business Application information listed in Asset Details comes from a CMDB pull and provides us relevant context on the way the asset is being used, who owns it and what department and business service it belongs to.

Business Information for the app includes the Business Criticality score assigned to it in ServiceNow. This is a text field and a user configurable score in ServiceNow. You can define how Business Criticality maps to the Asset Criticality Score in ServiceNow and CSAM automatically assigns these scores to the assets associated with the Business App in its inventory.

You can also see the list of assets associated with a business app which allows security teams to look for assets that have the biggest potential for impacting your business and ensure that they are properly secured.

Note: Only assets with the Qualys Cloud Agent installed show up under the “Associated Assets” tab withing a business application.

Use Business Attributes to Search Assets

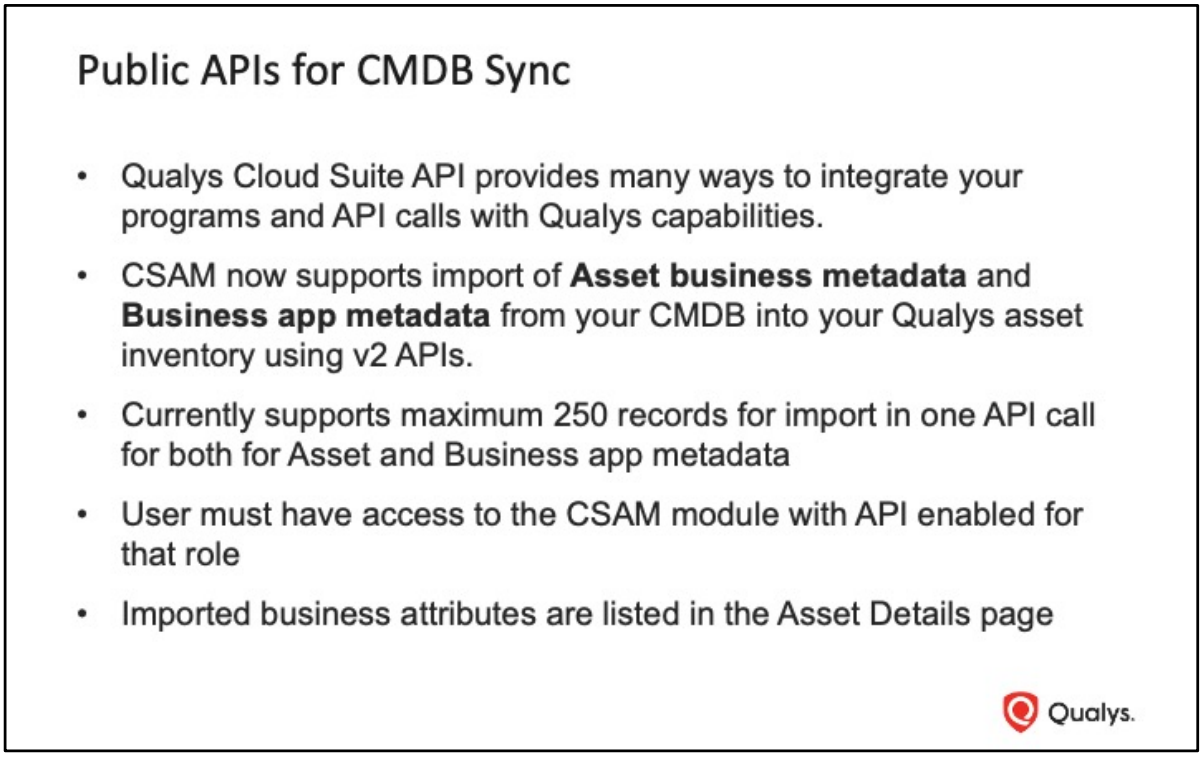


Use search tokens to filter assets matching specific business information

Qualys.

CSAM includes multiple search tokens to quickly filter assets matching specific business attributes that are imported from a ServiceNow CMDB sync.

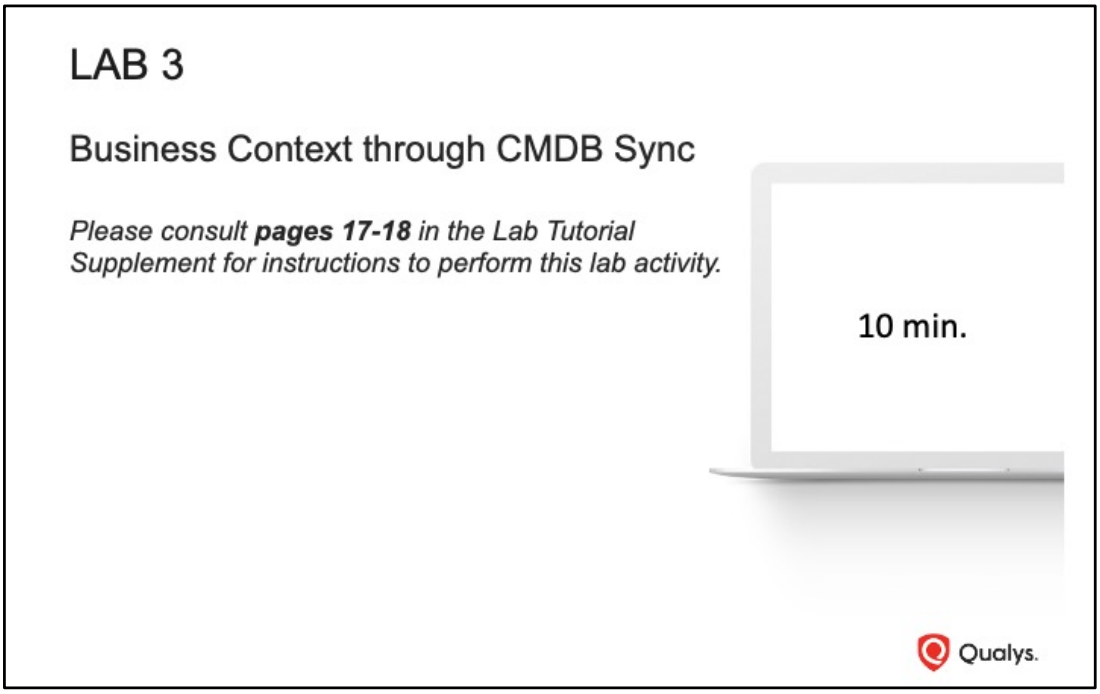
The slide illustrates a search query that looks for assets matching the highest Business Criticality Score (score 1 is the highest criticality score that is assigned in ServiceNow) AND associated with the 'Banking Service' application.



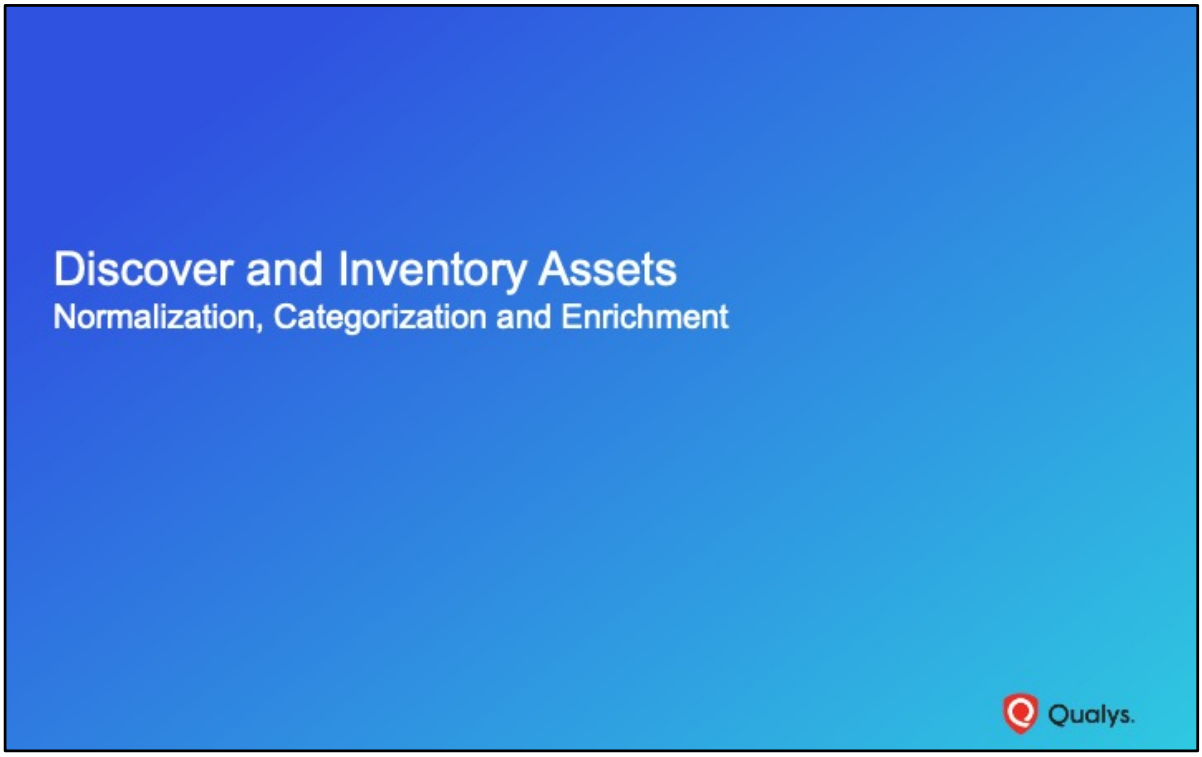
Qualys has added business information attributes support for the v2 APIs. You can now import **Asset business metadata** (eg: asset.org.company, asset.ownedBy, etc.) and **Business app metadata** (eg: businessApp.name, businessApp.businessCriticality, etc.) from your CMDB into your Qualys asset inventory in CSAM. A maximum of 250 records can be imported in one API call.

To use this feature, your account must include CSAM in the subscription. Also, the user making API requests must have access to the CSAM module with API access enabled.

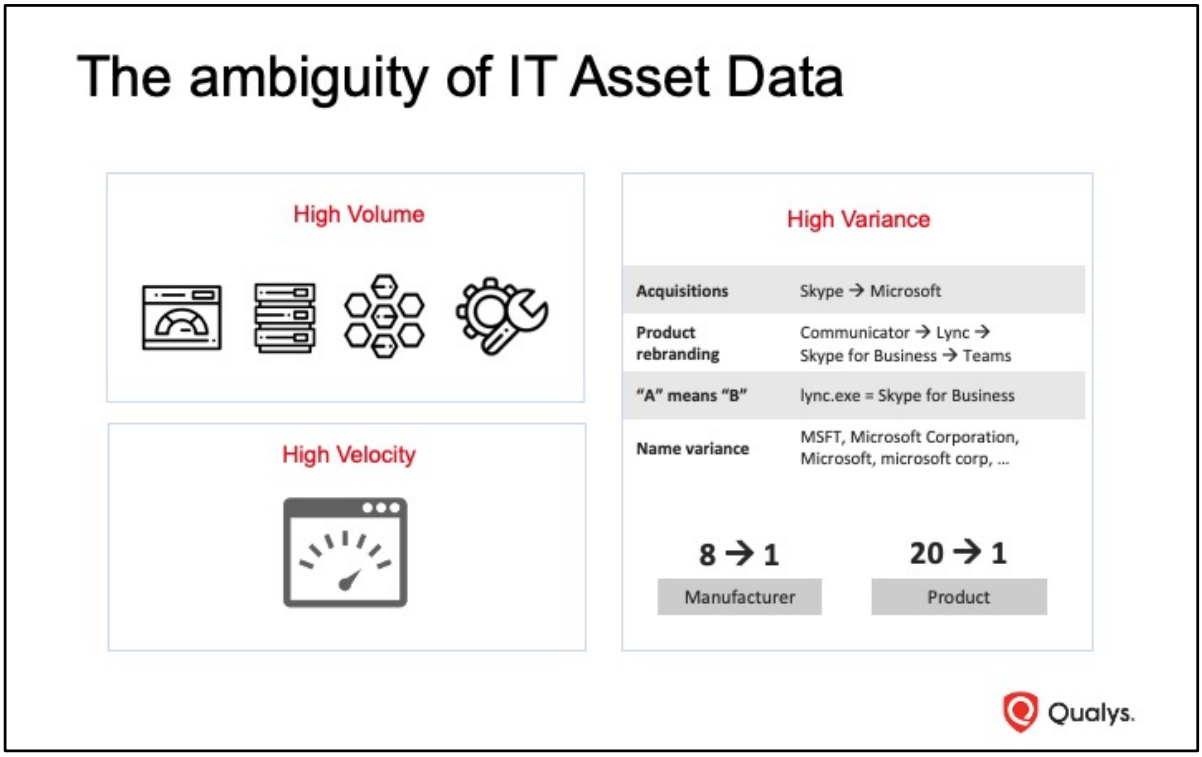
For more information on the business attributes supported for API requests, please consult the CSAM API Guide:
https://www.qualys.com/docs/qualys-gav-csam-api-v2-user-guide.pdf



Lab 3 will walk you through the steps to understand how security teams can get business context in CSAM with ServiceNow CMDB integration.



This topic provides an overview of the Global AV / CSAM capabilities of normalization, categorization and enrichment.



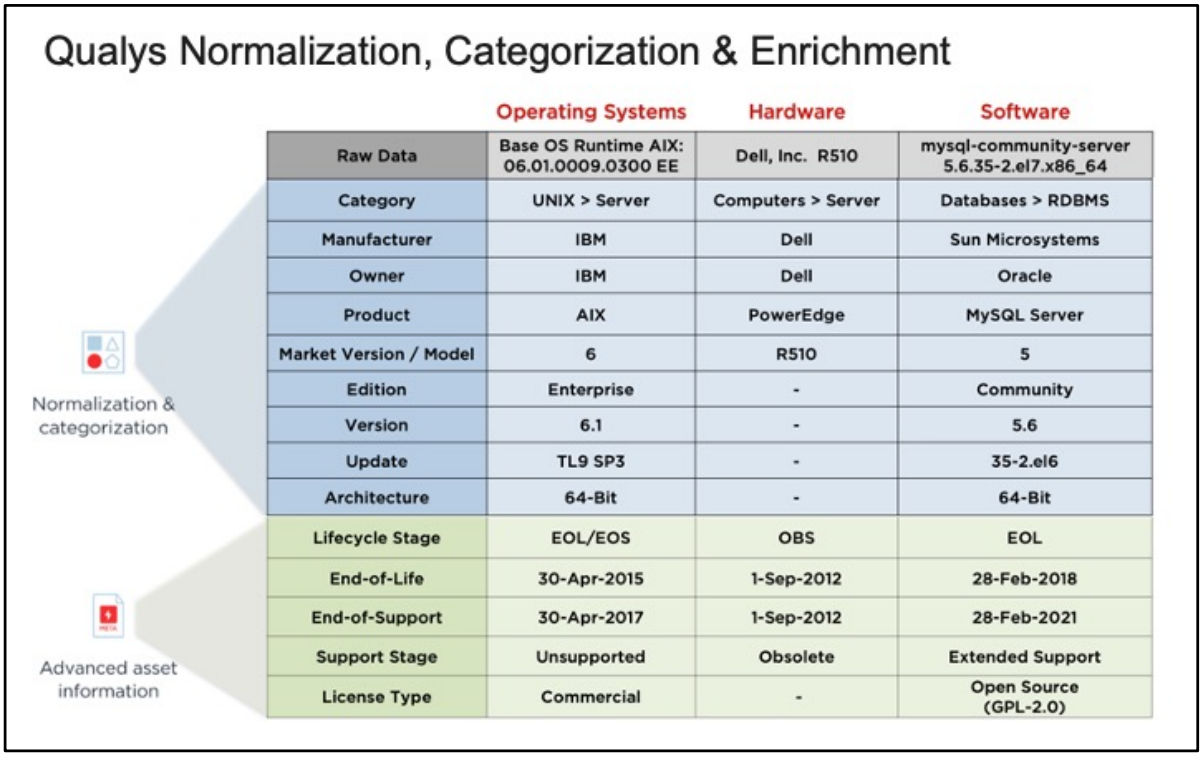
One of the biggest challenges when building an automated asset inventory is the volume, velocity and variety of asset changes in the environment.

This challenge is increased exponentially when organizations take full advantage of Cloud, which allows organizations to dynamically adjust workloads, such as compute resources delivered by virtual machines and containers.

Qualys tackles the Volume and Velocity challenges by providing a powerful Cloud Platform capable of processing asset telemetry in near real time, and then leveraging that same telemetry to solve multiple use cases for IT Asset Management, Security and Compliance through its family of integrated Cloud Platform Apps.

With Qualys GAV / CSAM, customers can tackle the High Variance challenge of asset data, and make their asset inventory consistent and uniform, which is essential for having inventory clarity and accuracy.

You have a high volume of data and vendors are constantly changing and rebranding themselves. This makes it difficult to categorize your data. Qualys has taken that idea and we normalize your information for you. So when Skype was acquired by Microsoft those products became Microsoft and we can categorize those things.

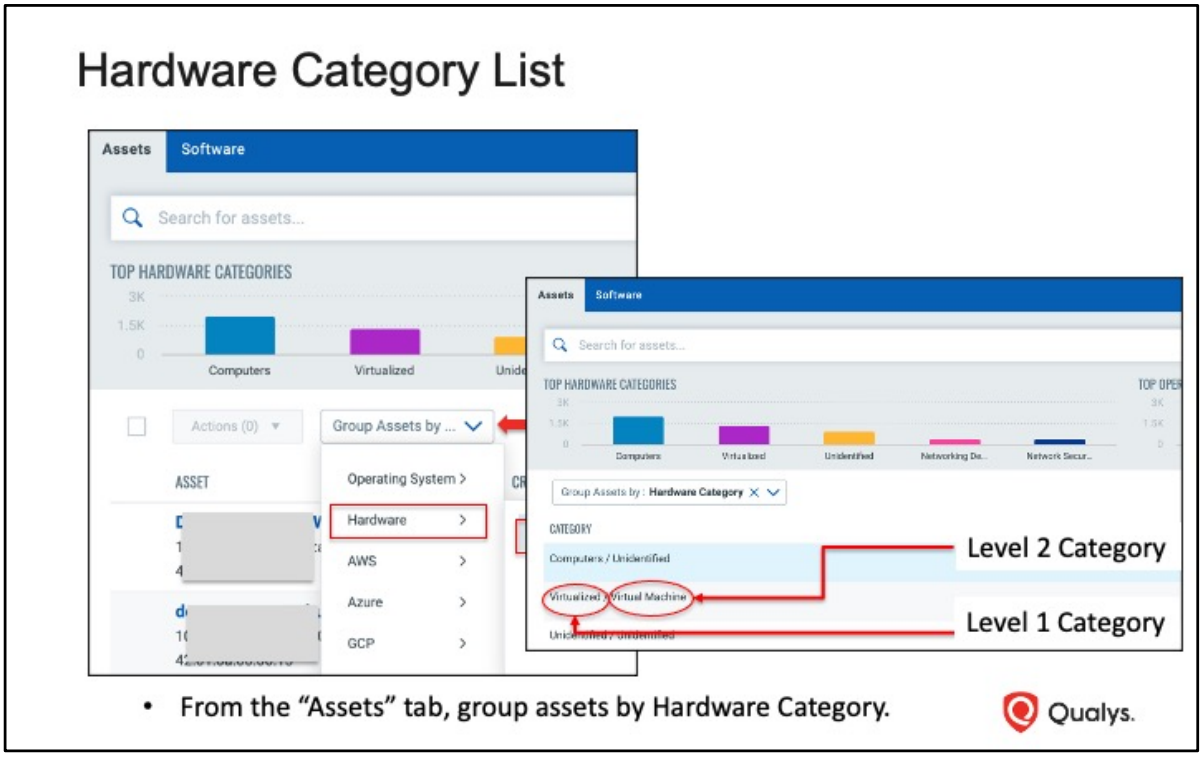


Raw Asset Data – We start with the raw asset data. This is the information that's collected from your sensors and sent to the platform.

Qualys normalization and categorization – here is where we take that data and we break it down by manufacturer, owner, product, Version, edition, and category. This happens after the data is retrieved using a sensor. Every standardized product in the technology catalog belongs to a 2-level taxonomy, for example "Computer / Server" or "Database / RDBMS", which helps organize all assets in multiple dimensions.

Enrichment – Finally we tell you if it's end of support and end of life, what type of license it has, and the risk associated with those things.

The catalog is continuously curated with a focus on completeness, relevance, and data quality. This process transforms the global IT asset inventory into a multi-dimensional and structured set of information, so that you can make better business decisions.



If you would like to identify all the hardware categories in your account, navigate to the "Assets" tab (within Global AV / CSAM) click "Group Assets by," and then select Hardware and then Category. The result will display all hardware instances categorized by their level 1 and 2 categories.

Hardware Classification

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

Qualys.

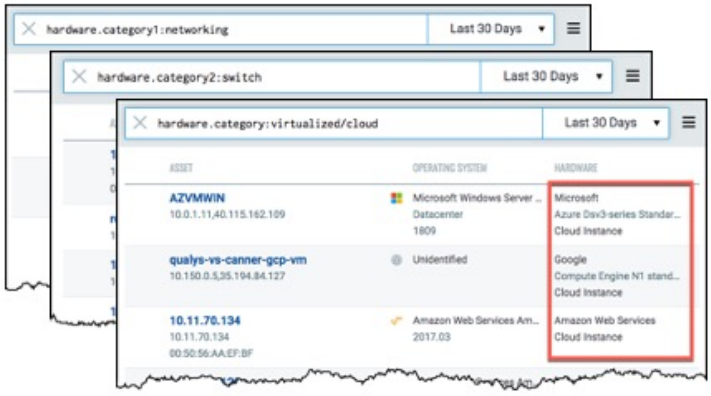
The hardware, operating system, and software categories can be handy when performing asset searches within the Global AV / CSAM application.

You can filter/sort assets in your organization based on the underlying hardware in various ways.

The table in the slide lists the available search tokens to filter assets by their hardware category, name, manufacturer, product, and model.

Search Hardware Categories

```
hardware.category1:value1
hardware.category2:value2
hardware.category:value1/value2
```



Qualys.

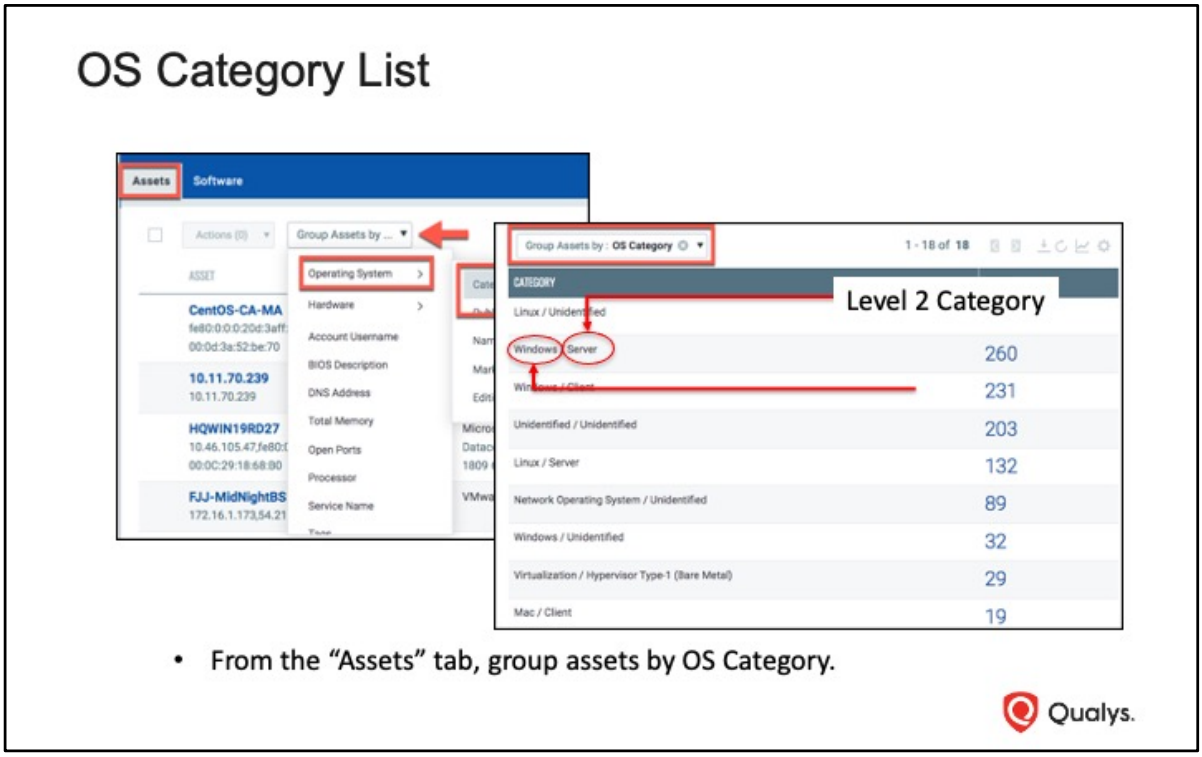
In this example, we're looking at hardware categories. To construct a query, identify a hardware category token, followed by a targeted value. You can use hardware.category1 and a category1 value, hardware.category2 and a category 2 value, or you can combine category1 and category2 using the "hardware.category" token (a slash character must separate the category1 and category2 values).

The first illustration depicts a “hardware.category1” query for all networking devices.

The second illustration depicts a “hardware.category2” query just for switch devices.

The third illustration depicts a plain “hardware.category” query for virtual devices that are cloud-based (notice the slash that separates the category1 and category2 values).

In a moment, We'll take a look at a simple way to identify all the hardware.category1 and 2 values in your account.



If you would like to identify all the OS categories in your account, navigate to the "Assets" tab (within the “Inventory” section) click "Group Assets by," select Operating System and then Category.

Operating System Classification

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

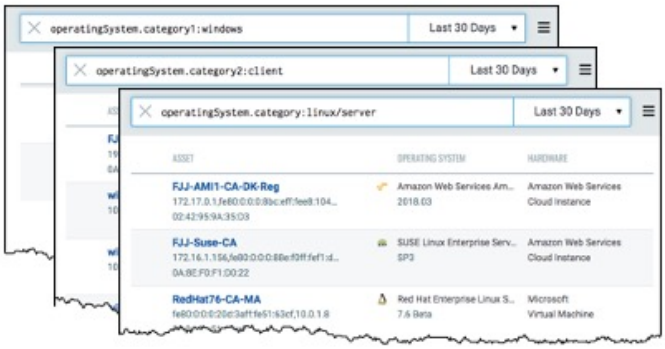
Qualys.

Similarly, you can filter/sort assets in your organization based on the installed OS in various ways.

The table in the slide lists the available search tokens to filter assets by their OS, OS category levels,, publisher, name, architecture, market version, update level and edition.

Search OS Categories

```
operatingSystem.category1:value1
operatingSystem.category2:value2
operatingSystem.category:value1/value2
```



Qualys.

In this example we have operating system categories.

OS category queries are similar to the hardware category queries illustrated in the previous slides.

The first illustration depicts an “operatingSystem.category1” query for Windows assets.

The second illustration depicts an “operatingSystem.category2” query just for client hosts.

The third illustration depicts a plain “operatingSystem.category” query for Linux-based servers (notice the slash that separates the category1 and category2 values).

Software Category List

- From the “Software” tab, group software by Category.

Qualys.

If you would like to identify all the Software categories in your account, navigate to the ”Software" tab (within the “Inventory” section) click "Group Software by," and select Category.

Software Classification

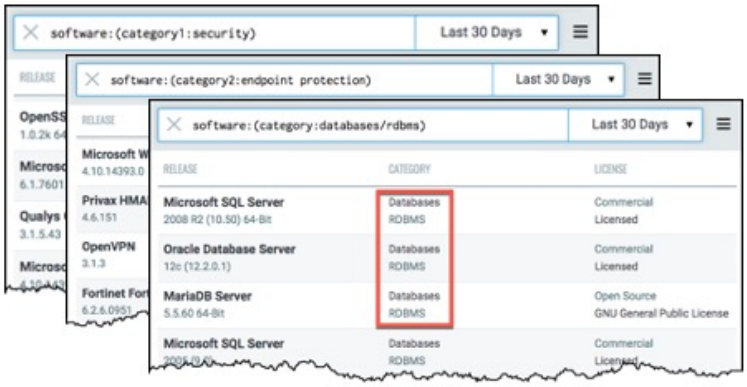
Attribute	Examples	Search Token
type	Application, Driver, OS Update, Unknown	software.type
category (level1 / level2)	Productivity > Productivity Suites	software.category
category (level1)	Productivity	software.category.1
category (level2)	Productivity Suites	software.category.2
full software name	Microsoft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

You can also filter/sort the software in your organization in various ways.

The table in the slide lists the available search tokens to filter software by their type, category, name, publisher, product, architecture, market version, software version, update level and edition.

Search Software Categories

```
software:(category1:value1)
software:(category2:value2)
software:(category:value1/value2)
```



Qualys.

Category 1- Applications are categorized within a first level category, e.g. Databases, Security, Productivity, etc. Basically, what type of application is this?

Category 2 - Each Application category is then further classified in subcategories, for example Security into Endpoint Protection, Authentication, Data Loss Prevention, Browser, etc.

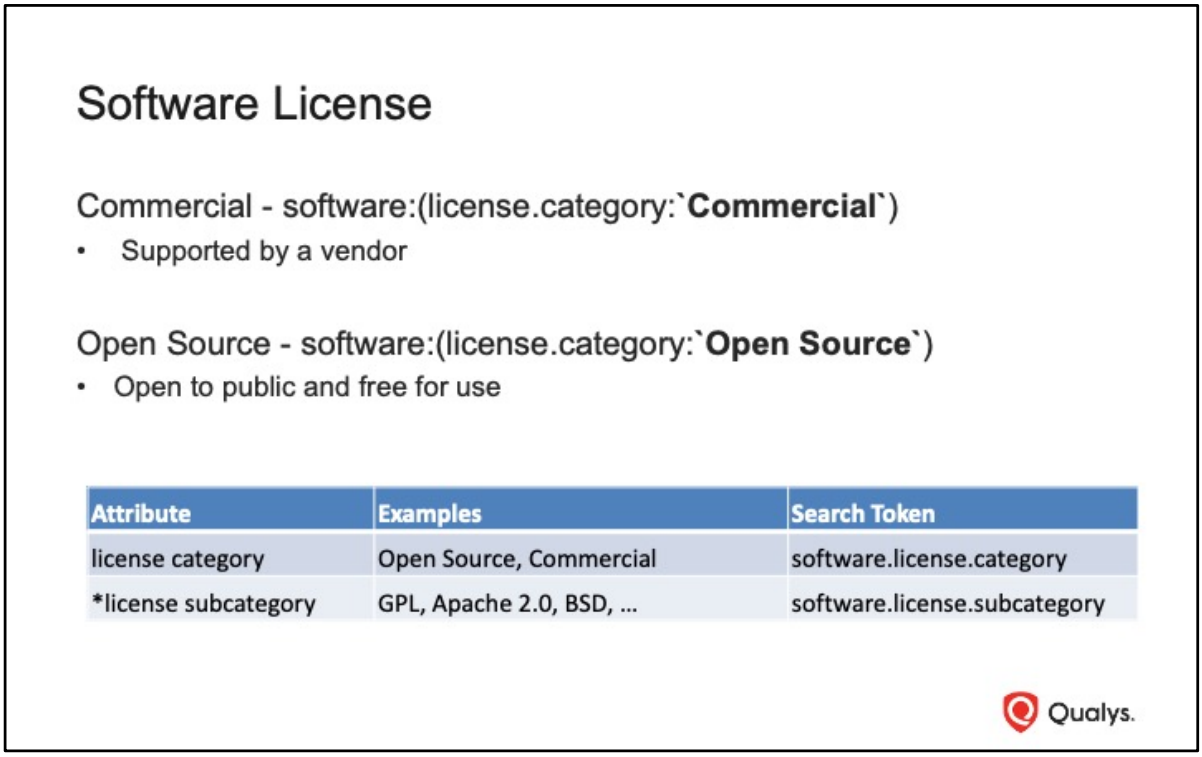
Software category queries are also like hardware and OS queries, with one small exception.

Notice the parenthesis that surround the category and value.

The first illustration depicts a “software:(category1” query for security applications.

The second illustration depicts a “software:(category2” query just for endpoint protection applications.

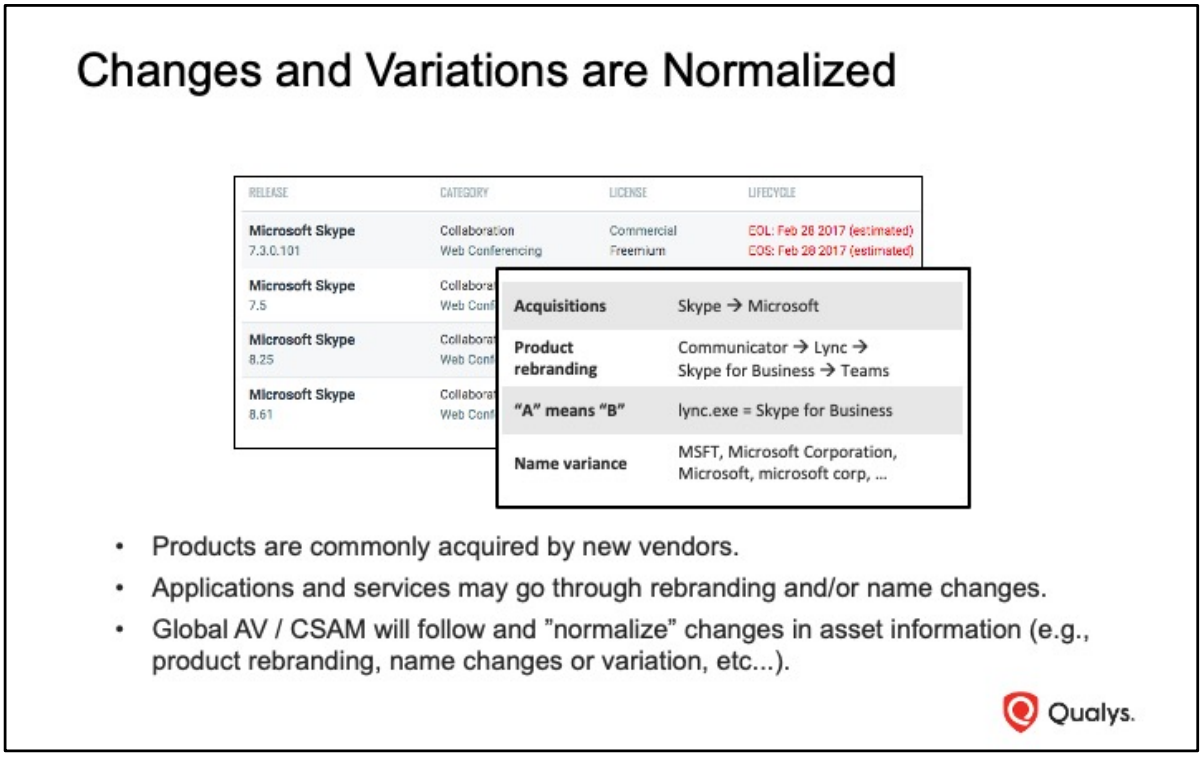
The third illustration depicts a plain “software:(category” query for relational database management systems (notice the slash that separates the category1 and category2 values).



Find your commercial vs open-source software.

Why does this matter? If you look an environment, you can see millions of software deployed. If you are in IT, you are trying to look at spend, or potential locations to save money when not using certain licenses (under utilized software).

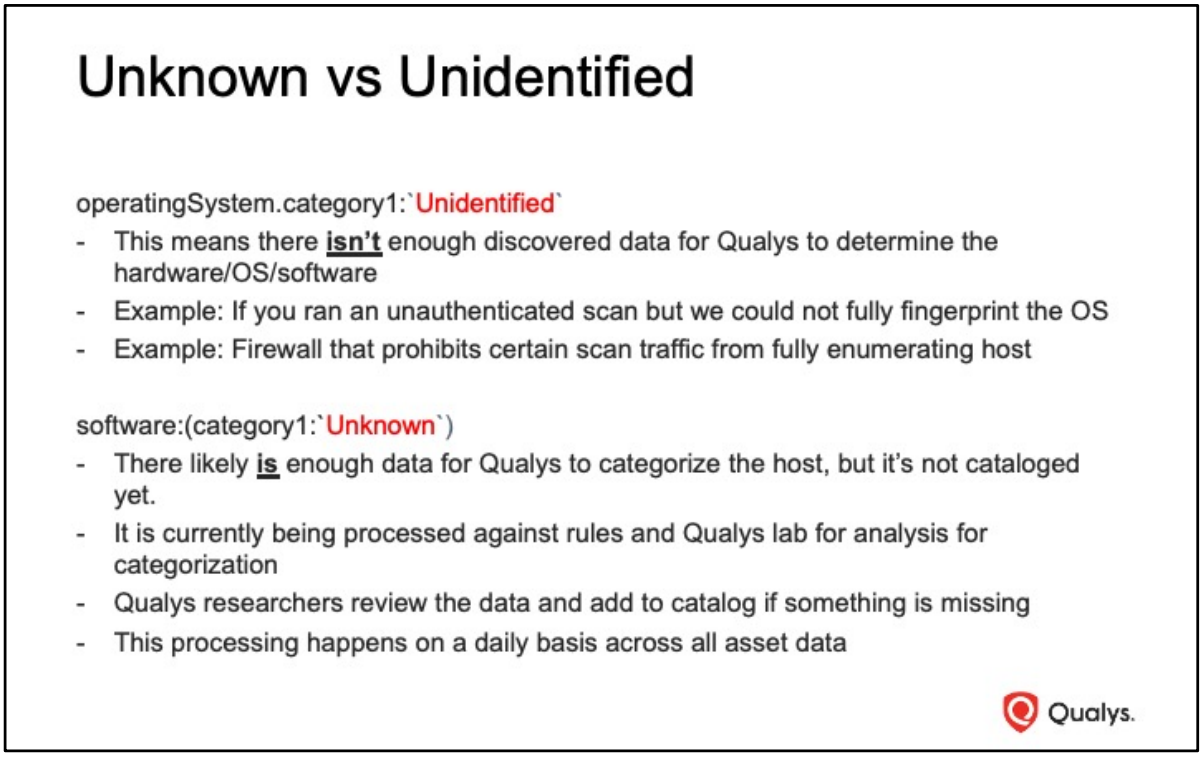
Because we are categorizing, quickly gives you insight into all commercial software.



It is also common for products to undergo rebranding or name changes throughout their lifespan. This illustration depicts the name changes and rebranding that occurred, when Microsoft acquired Skype. **Skype for Business** (formerly **Microsoft Lync** and **Office Communicator**) was eventually discontinued in in favor Microsoft Teams.

Even without rebranding or name changes, some products simply have variations in the names that are used to identify them.

Global AV / CSAM is designed to recognize these changes and variations and make any necessary adjustments.

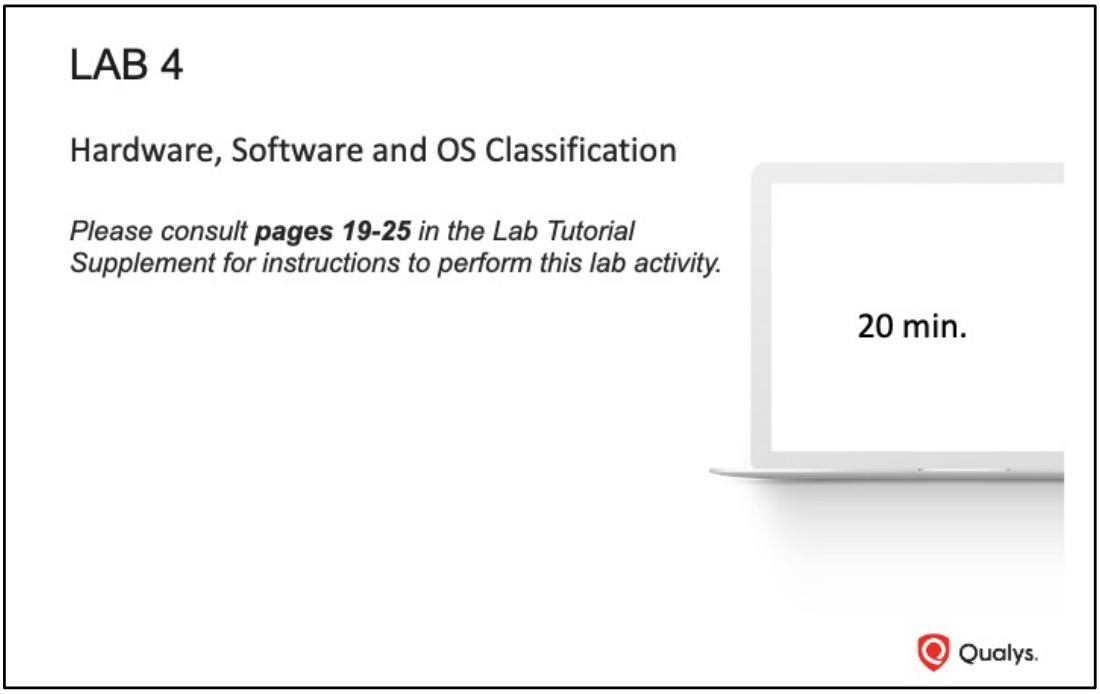


When you see something show up in GAV / CSAM as unidentified, it means that we do not have enough data that allows us to determine what the hardware/software/OS is.

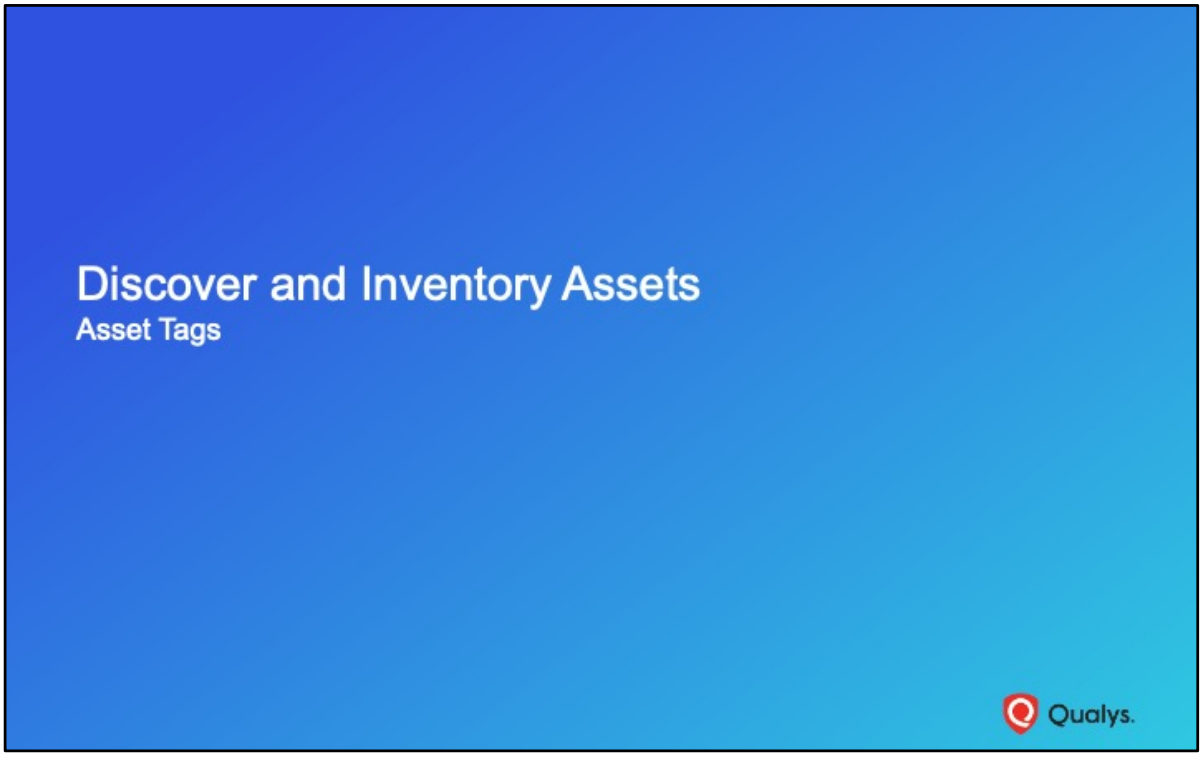
If you see something as unknown, then it means Qualys has not categorized the host, but we do have enough data. This means the data is currently being processed in the Qualys lab and usually are able have a categorization within several days.

This slide also highlights the difference between AssetView (legacy) and GAV / CSAM:
In AssetView, everything is unidentified and unknown. There is no categorization. No license categories. No hardware, software, or OS categories.

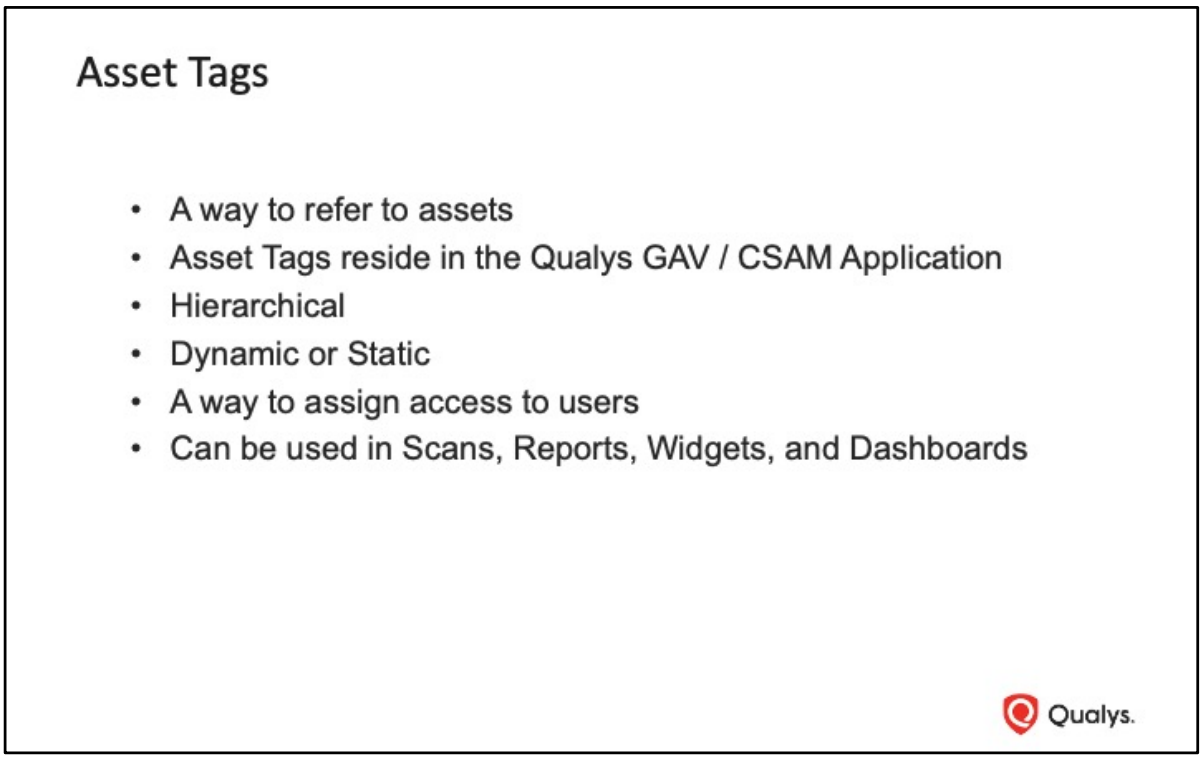
In GAV / CSAM, we add the structure of Categorization, Normalization, and Enrichment.



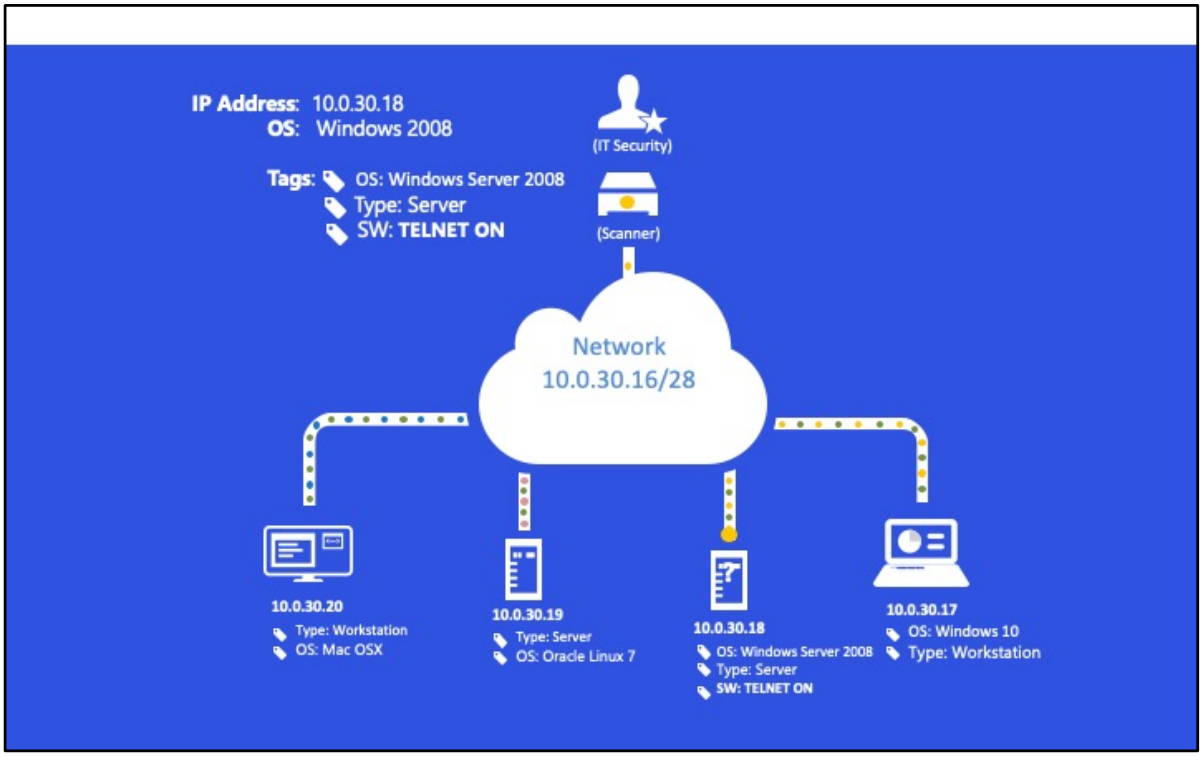
Lab 4 will walk you through the hardware, OS and software categorization feature in CSAM.



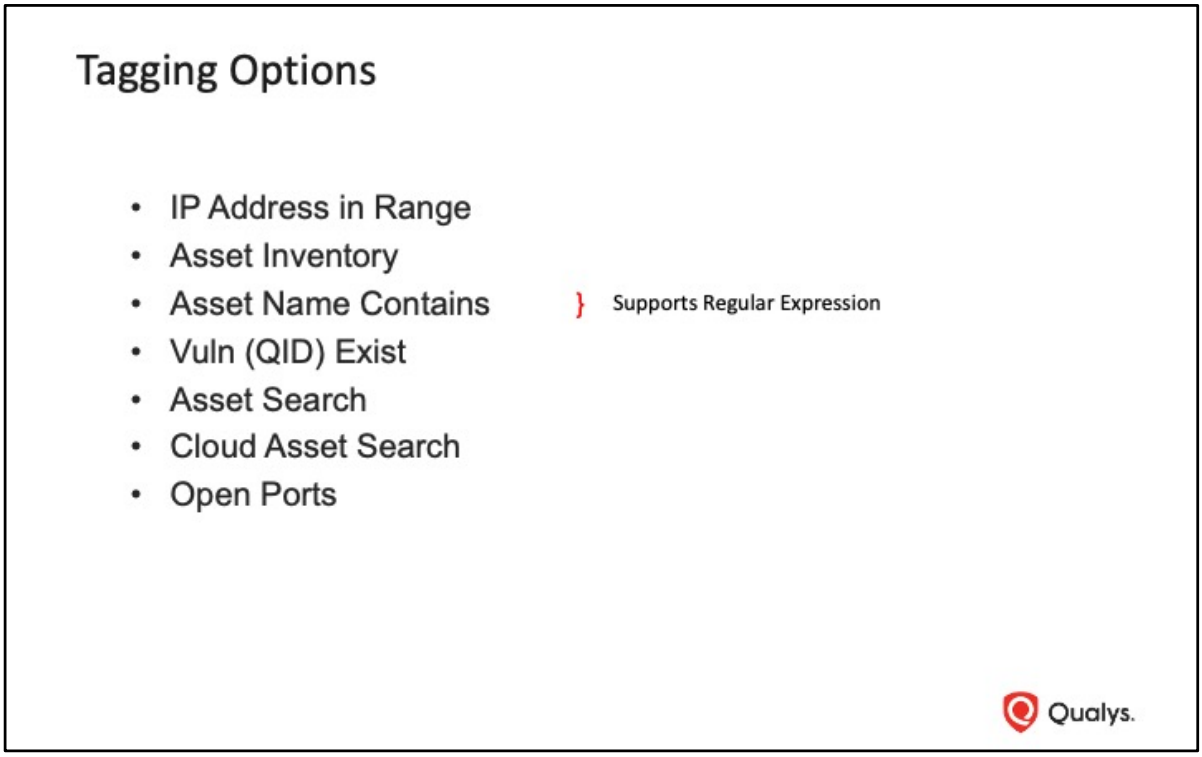
Next, we will understand how to setup static and dynamic Asset Tags.



Dynamic asset tags update automatically based on the attributes of the asset. The data required for tags to be updated is provided by Qualys scanner appliances, cloud agents and cloud connectors.

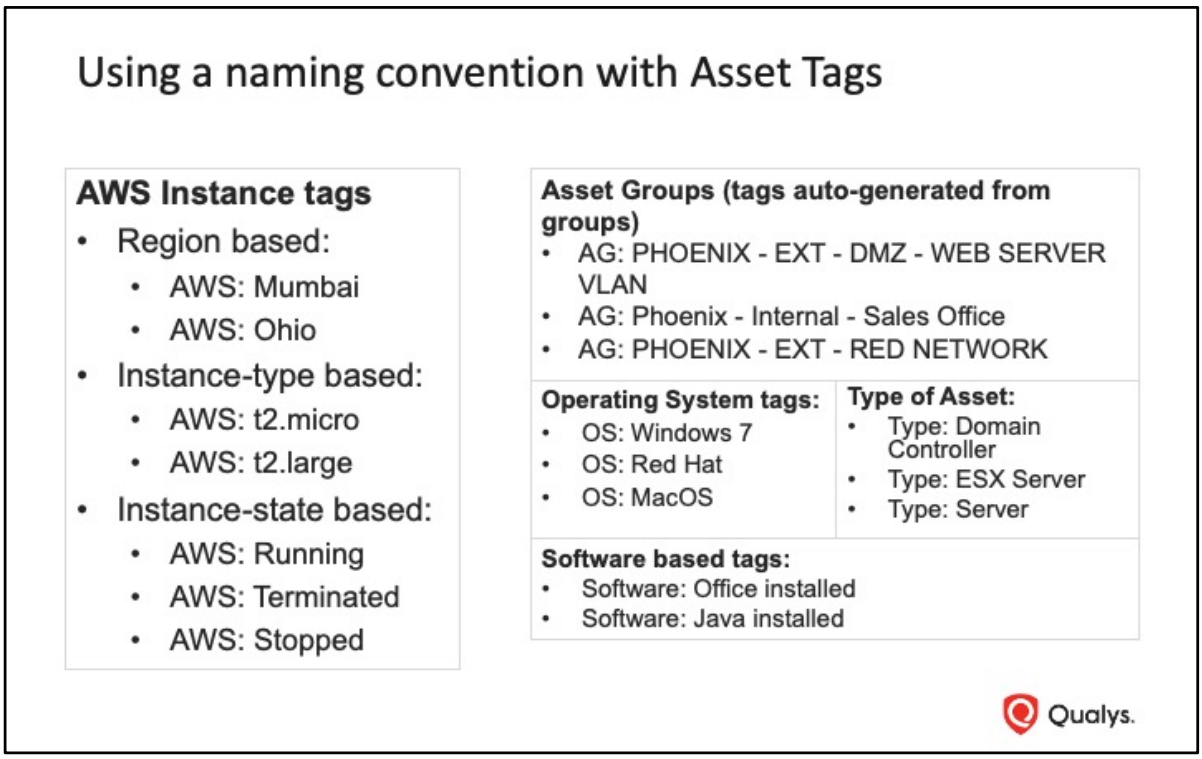


This is an illustration of how data collected from the assets is used to populate the tags.



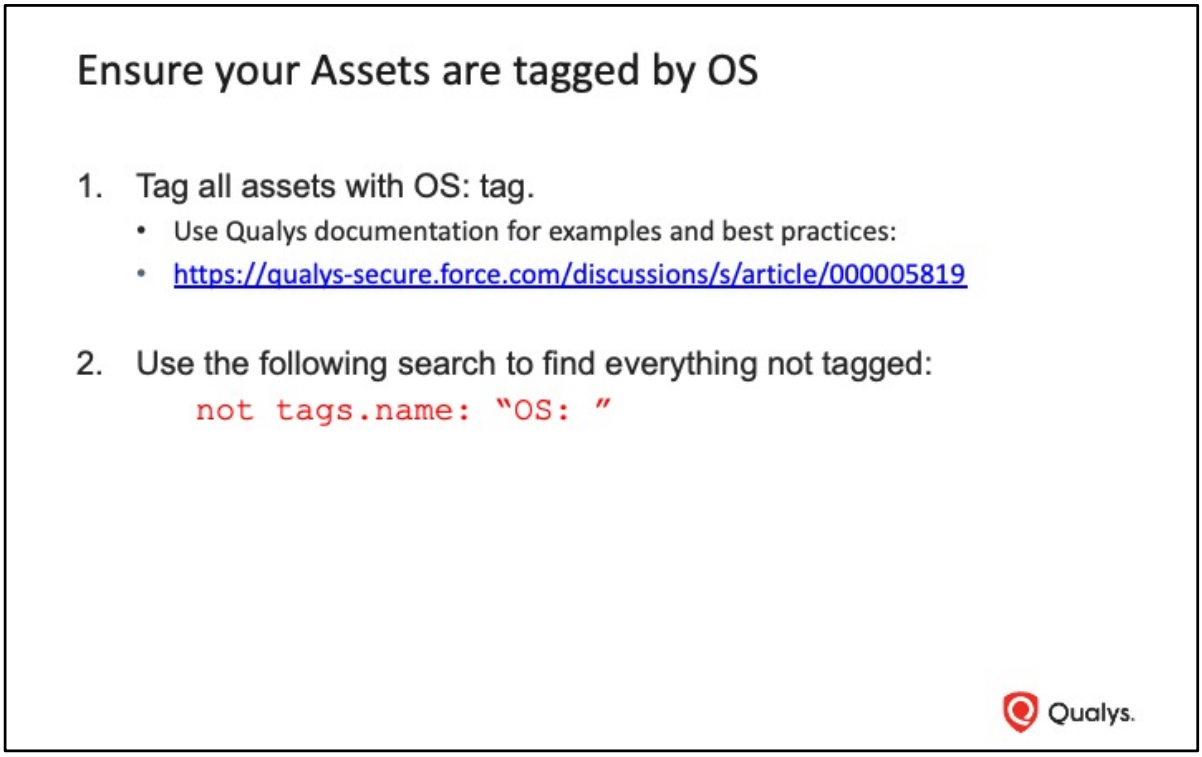
Dynamic Asset Tags are created using various types of Asset Tag Rule Engines. The slide lists the available options for setting up dynamic tag rules.

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



It is important to following a standard naming convention for your asset tags. This will make it easy to organize and search for them.
Examples:
- Type: Domain Controller
- SW: iTunes
- OS: Ubuntu

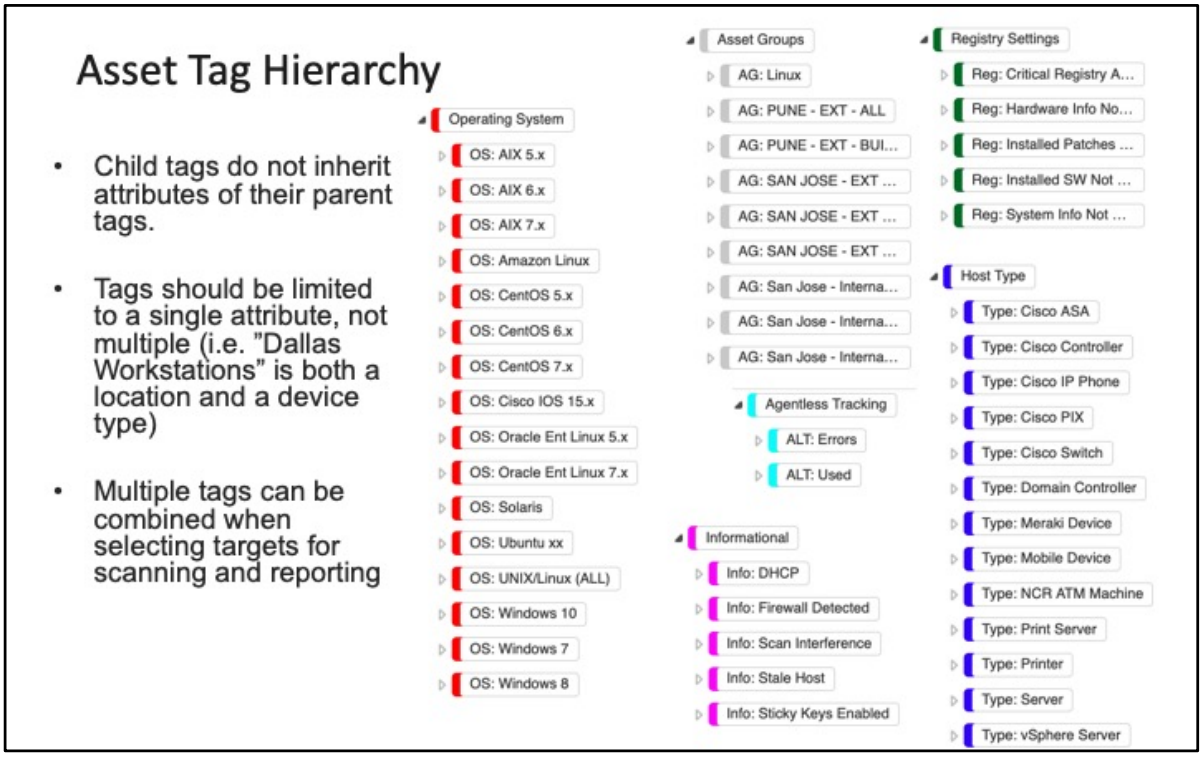
Here you see examples of tags. It helps you easily query for and find assets with a particular tag.



Choose tag names that are descriptive, but brief.

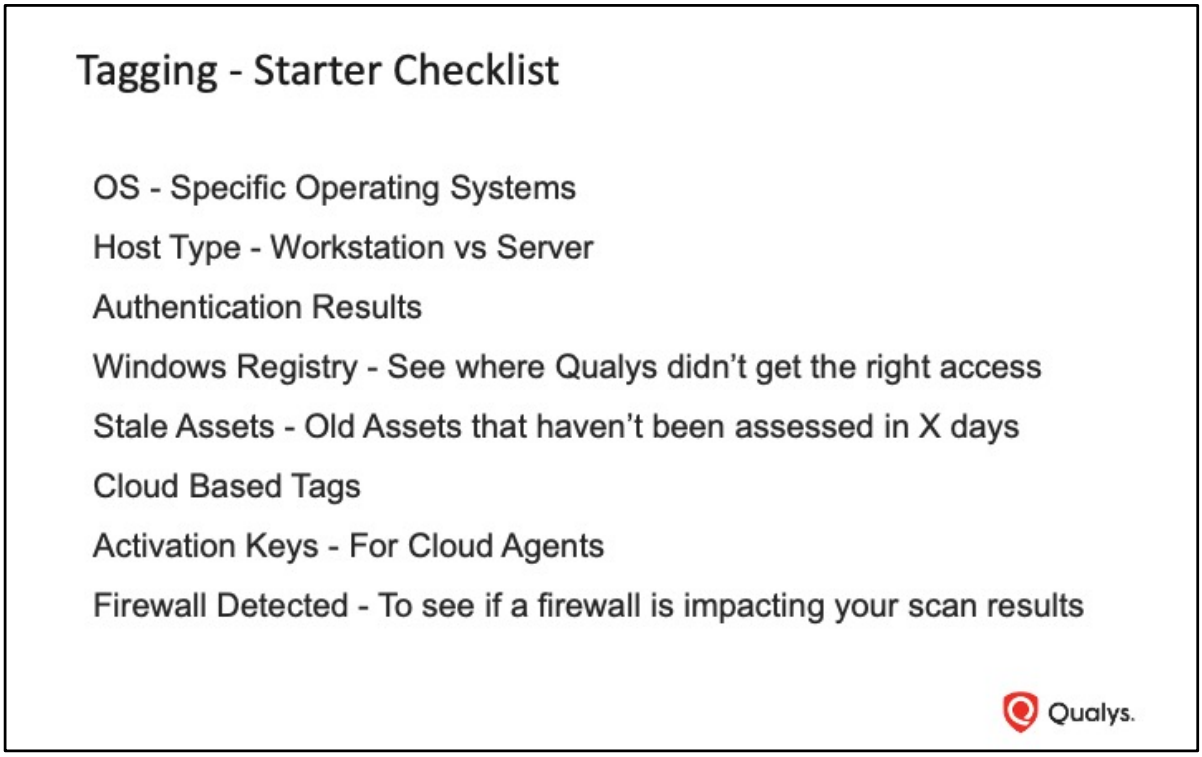
To help organize Asset Tag hierarchies, avoid mixing multiple types of rule engines in a single hierarchy.

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

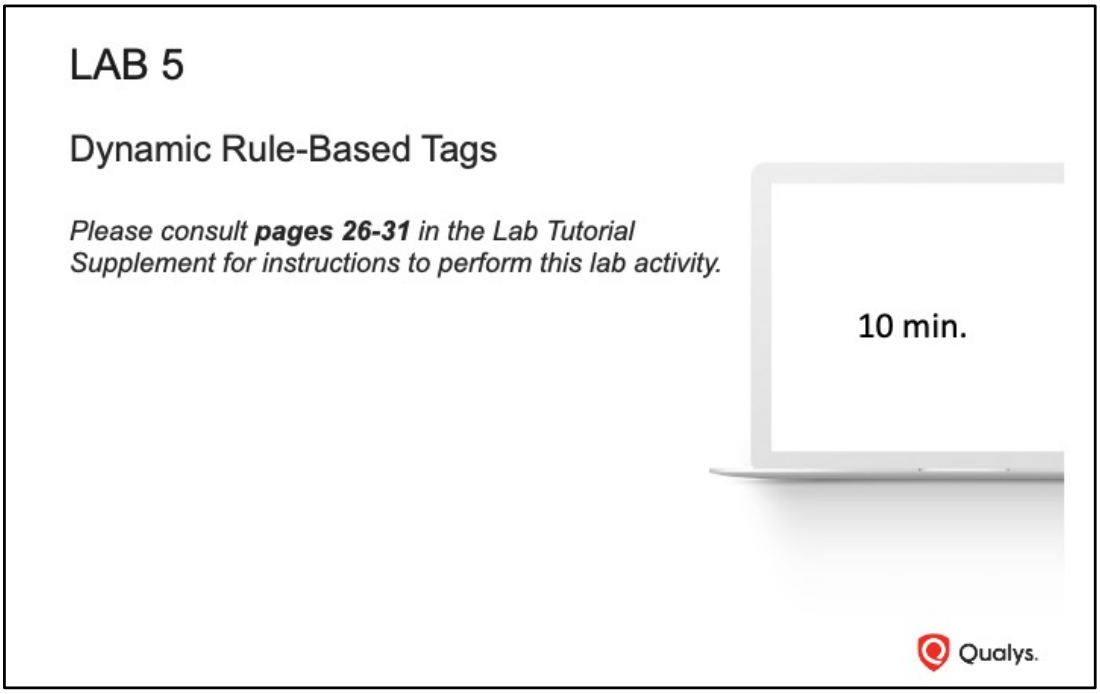


You end up with a tagging hierarchy that looks something like this.

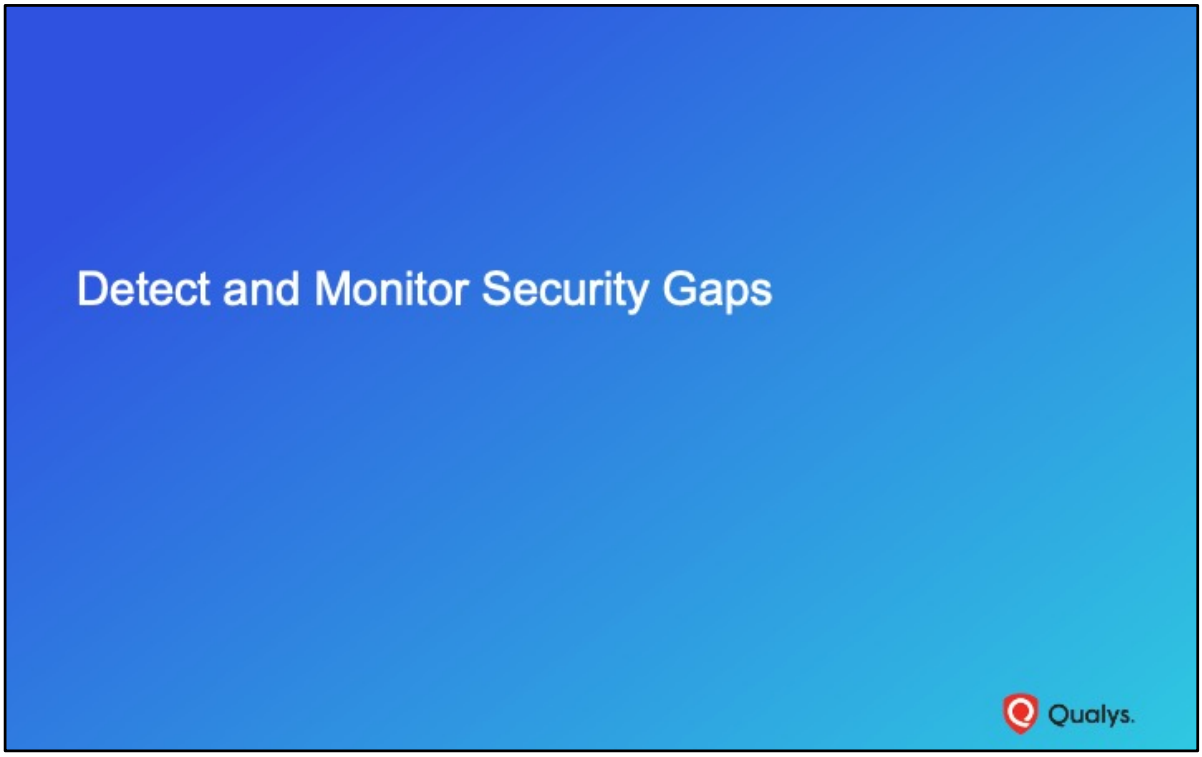
In doing this, you've set the foundation for tagging and made things easier to sort and filter later, when it comes time to build your dashboards, widgets, and reports.



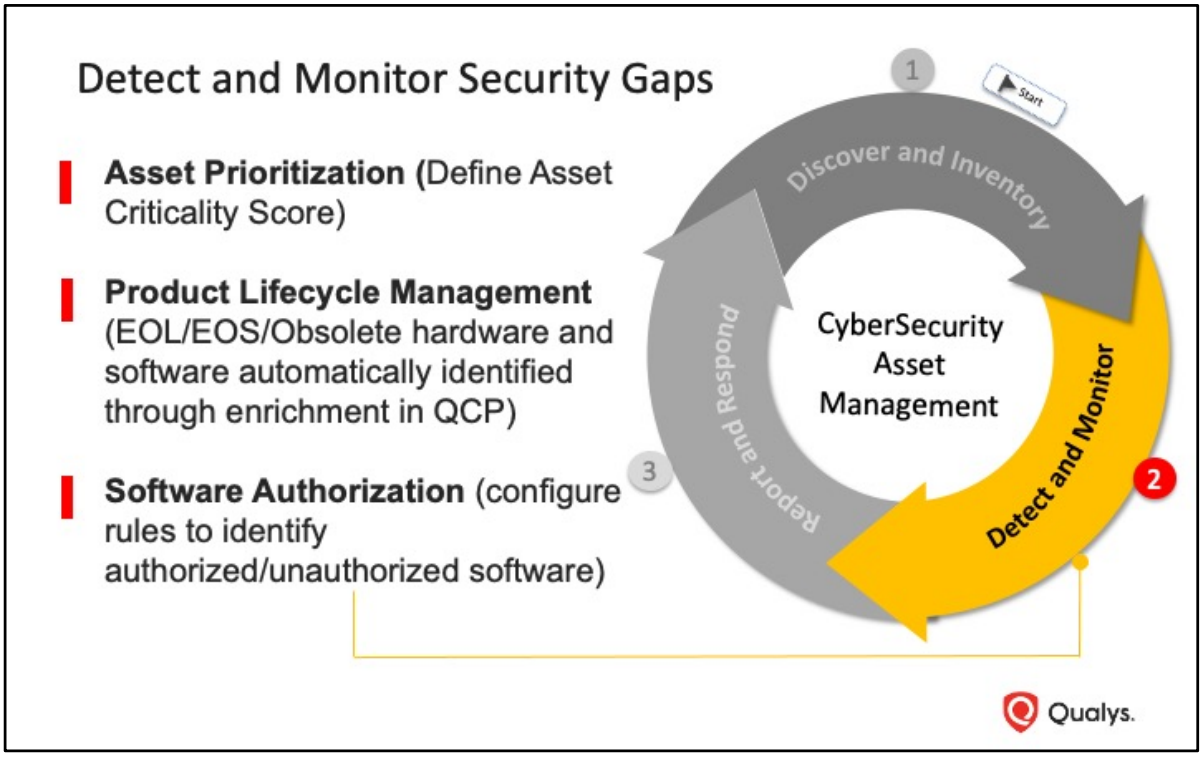
OS specific – This will allow you to build reports with tags that are specific to an operating system. Most organizations want to report based on OS.
Device type – This is so you can filter reports and dashboards based on servers or workstations, and evaluate risks at the device type level
Auth Record – By tagging auth records, you can see which ones are being used
Windows Registry – This will allow you to troubleshoot devices where Qualys didn't have the right access.
Stale Assets – You can filter out assets that haven't been scanned in X days from your reports
Cloud Based Tags – Any asset deployed in AWS, GCP, Azure can be tagged in a variety of ways and often needs to be separate from your corporate environment
Activation Keys – This is so you can track assets with agents provisioned out of given centers, and report on Cloud Agent assets specifically
Firewall Detected – This is so you can see if there may be a firewall impacting the scan you're running.



Lab 5 will walk you through the steps to create dynamic Asset Tags in the CSAM application.

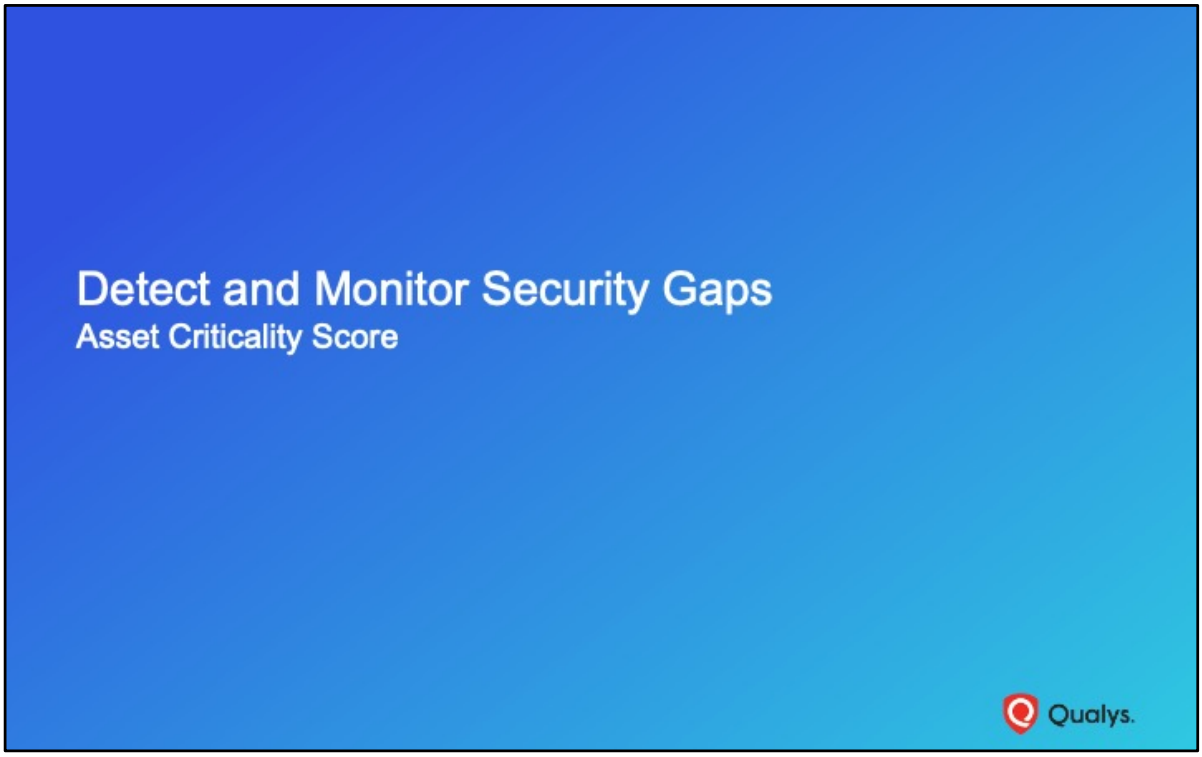


This section provides an overview of the steps to configure Asset Criticality Score on Asset Tags.



Detect and Monitor

In the next step (step 2), you can detect unsupported hardware, OS and software, identify unauthorized software and use Asset Criticality Scores to prioritize assets for response.



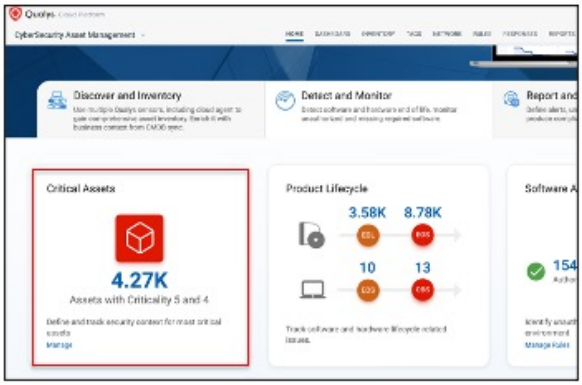
This topic provides an overview of the steps to configure Asset Criticality Score on Asset Tags.

Asset Criticality

Define a key business context that allows organizations to prioritize security assessment and remediation actions.

Features

- Asset Criticality Score (1-to-5) optionally assigned to Asset Tags
- Assets are then assigned the highest criticality score aggregated across all tags that are applied to the asset
- Search by Asset Criticality
- Create Dashboards with filters & group-by Asset Criticality
- Visible in GAV/CSAM & later VMDR



Note: This capability is available with Global AssetView, free for all customers.

Qualys.

Global AssetView and CyberSecurity Asset Management allow you to establish the relative business importance of an asset or software using an Asset Criticality Score (ACS). 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.

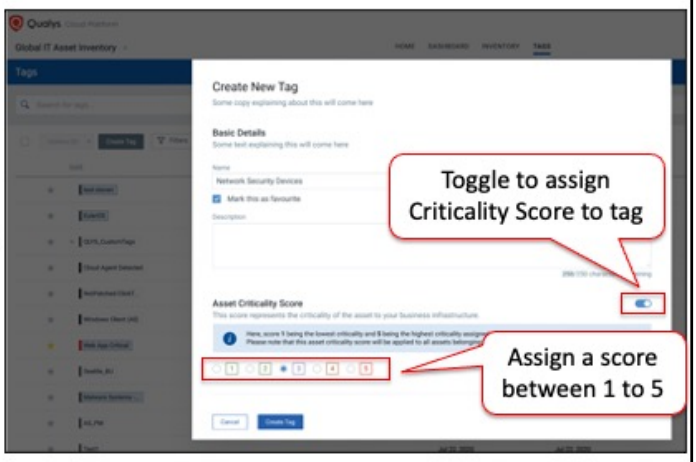
Asset Criticality is a user defined measure that enables the assignment of a criticality score to assets. The user optionally selects a criticality score on an Asset Tag which is then applied to one or more assets. An asset attribute is assigned the highest criticality score among allocated asset tags.

If pulling data from ServiceNow CMDB (supported only in CSAM), the Asset Criticality Score is automatically calculated from the Business Criticality score assigned to the asset in ServiceNow.

Assigning Criticality Scores

Asset Criticality Scores are:

- User defined scores
- Assigned on a scale of 1 to 5
- Implemented through Asset Tags



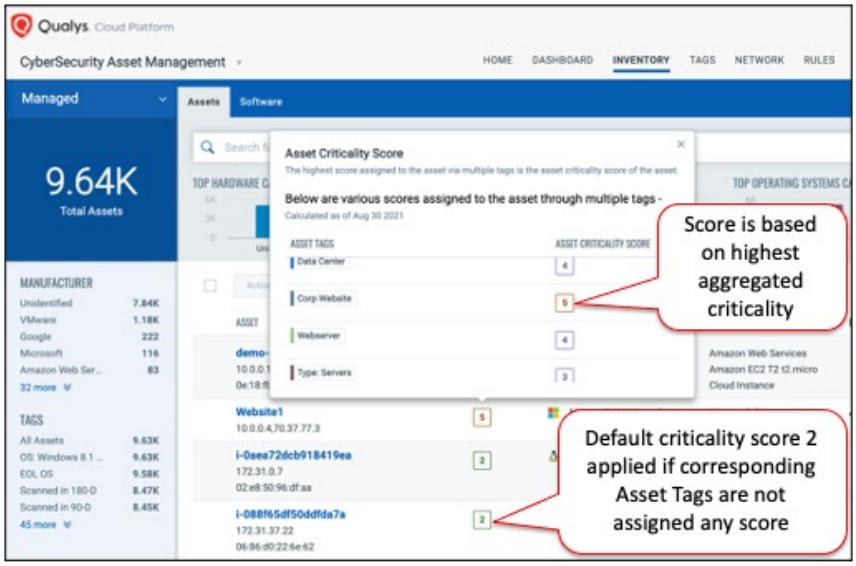
Qualys.

Asset Criticality Scores are implemented through our static and dynamic Asset Tags.

Asset Criticality Score setting is turned off by default for a tag. And the corresponding assets are assigned a default Criticality score of 2. You can change the default setting and assign a criticality score between 1 to 5 to the Tag.
Your production or business critical assets such as Order Management System devices or executive team laptops should generally be assigned a high criticality score of 4 or 5 while non-critical assets should be assigned a lower score.

Once you've created tags with Asset Criticality Score and tags are assigned to the asset, the Asset Criticality Score of the asset will be calculated.

Asset Criticality Score Calculation



Qualys.

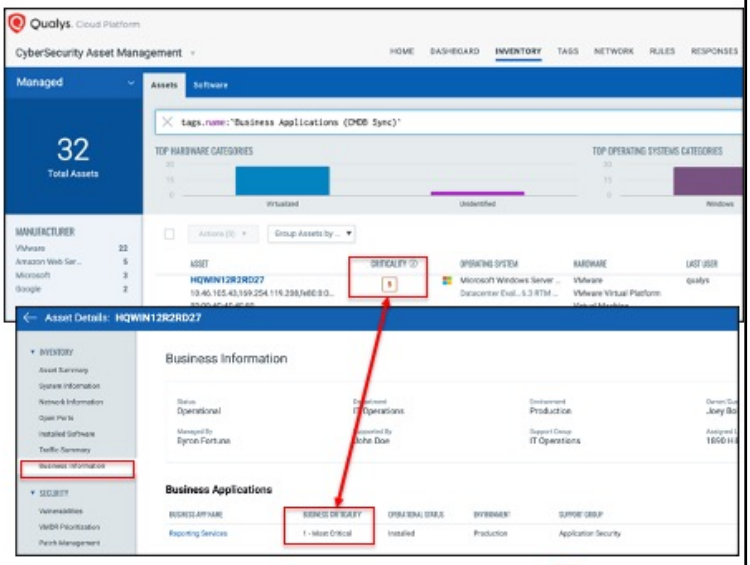
The INVENTORY section displays all assets where Qualys has collected data. Clicking on the Criticality score of an asset displays all the Asset Tags assigned to the asset along with their configured Criticality Scores. The Asset Criticality Score (ACS) is automatically calculated based on highest aggregated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

Mapping Business Criticality to Asset Criticality Score

- CMDB Sync enriches Qualys asset inventory with key CMDB business data
- CSAM automatically maps Business Criticality score assigned to the Business App in ServiceNow to the appropriate Asset Criticality Score for the corresponding assets



By integrating with ServiceNow CMDB (available in CSAM), you can enrich Qualys asset inventory by importing relevant business context, such as asset owner, environment, business applications and other key data into CSAM to improve response to asset health issues. Note that CMDB Sync must be configured for your Qualys account which is done using our ServiceNow-certified CMDB Sync App.

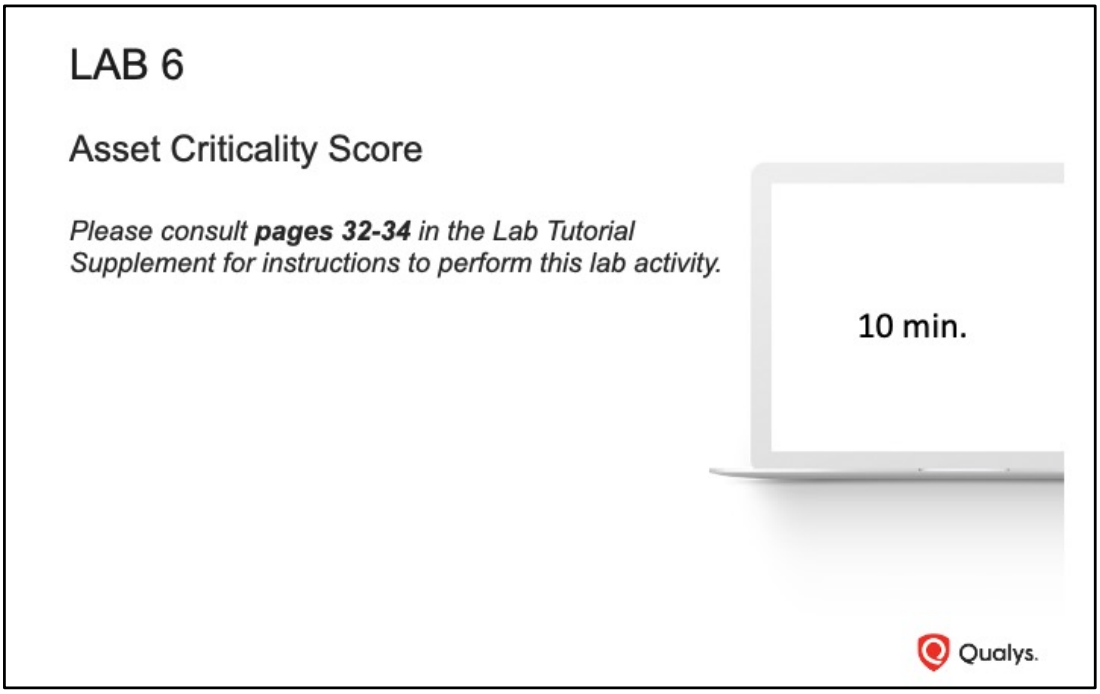
The Business Information and Business Application information listed under Asset Details for an asset comes from a CMDB pull. This provides us relevant context on the way the asset is being used, who owns it and what department and business service it belongs to. Here you see Business Information for the app including the Business Criticality score assigned in ServiceNow.

Note that Business Criticality scores follow a different prioritization scheme than the Asset Criticality Scores in CSAM. You can define how the Business Criticality Score maps to the Qualys Asset Criticality Score in ServiceNow.

Following a CMDB sync, CSAM automatically maps these Business Criticality scores assigned to the Business App to the appropriate Asset Criticality Scores to the assets mapped to the business app in Qualys inventory.

By bringing this Business Service data into Qualys, CSAM allows you to look for assets that have the biggest potential for impacting your business and ensure that they are

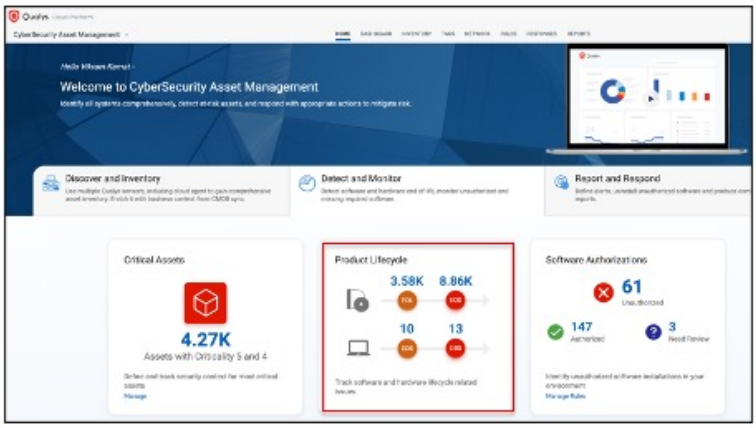
properly secured.



Lab 6 will walk you through the steps to configure Asset Criticality Scores on Asset Tags.

This section provides an overview of the product lifecycle management feature in CSAM.

Identify Unsupported Software and Hardware



- Identify EOL/EOS software and hardware
- Plan hardware refresh and software upgrades
- Secure your environment by eliminating unsupported software and hardware

Qualys.

End-of-life (EOL) or End-of-Sale (EOS) is an expression commonly used by software and hardware vendors respectively to indicate that a product or version of a product has reached the end of usefulness in the eyes of the vendor. And End-of-Support (EOS) or Obsolete (OBS) is an expression used by software and hardware vendors respectively to indicate when a product is no longer serviced via upgrades, patches, or maintenance.

Many vendors announce the EOL/EOS/OBS dates for their products far in advance.

EOL/EOS/OBS software and hardware are exposed to vulnerabilities that may be exploited by attackers.

On the CSAM HOME page, you can get a snapshot of all your software and hardware lifecycle information in one place.

With CSAM, we automatically apply our extensive EOL/EOS/OBS product catalog to your IT inventory, highlighting not only current hardware and software that are end of life and end of support/obsolete, but instances that are getting ready to reach that milestone and giving you the ability to proactively plan for addressing this security risk.

Hardware Lifecycle Stage

Search Token: `hardware.lifecycle.stage:value`

- **General Availability** (GA) - Hardware is in production, available for purchase, and supported
- **End of Sale** (EOS)- No longer being sold or by vendor
- **Obsolete** (OBS) - End-of-Service; no longer serviced via upgrades, patches, or maintenance

Qualys.

The Lifecycle stage information for hardware includes: General Availability, End of Sale, and Obsolete (which is equivalent to End of Service).

The term "Obsolete" was chosen, because the acronym for End of Service (EOS) is the same as End of Sale, which would create a conflict.

Values for the hardware.lifecycle.stage token include: EOS, GA, INTRO, Not Aplicable, OBS, Unknown

Hardware Lifecycle Search Tokens

Attribute	Examples	Search Token
lifecycle stage	"INTRO", "GA", "EOS", "OBS"	hardware.lifecycle.stage
Introduction date	Feb-2015	hardware.lifecycle.intro
General Availability date	Apr-21-2014	hardware.lifecycle.ga
End-of-Sale date	May-2016	hardware.lifecycle.eos
Obsolete date	Jun-2018	hardware.lifecycle.obs

Qualys.

CSAM currently has lifecycle information for over 100 hardware manufacturers and over 45,000 models. And these numbers are subject to change as Qualys continuously adds new hardware manufacturers, products and models to its catalog.

The slide lists the available search tokens in CSAM to identify hardware lifecycle information. Below is the explanation of the terminology used when referring to hardware lifecycle stages in CSAM:

INTRO

The hardware is in intro or trial phase

GA (General Availability)

The hardware is in production, available for purchase, and supported

EOS (End of Sale)

No longer being sold by vendor

OBS (Obsolete)

When it's no longer serviced via upgrades, patches, or maintenance

Note: Regarding lifecycles, CSAM has 10 to 20 times more lifecycle information than what you would find in QIDs.

OS & Software Lifecycle Stages

Search Tokens:

`operatingSystem.lifecycle.stage:value`

`software:(lifecycle.stage:value)`

- **Generally Available** (GA) - When the product became available for purchase.
- **End-of-Life** (EOL) - No longer marketing, selling, building new features, or promoting product (Security patches may still be provided).
- **End-of-Service** (EOS) - No longer serviced via upgrades, patches, or maintenance.

Qualys.

OS & SOFTWARE LIFECYCLE

General availability (GA) - When the product became available for purchase.

End-of-Life (EOL) - No longer marketing, selling, building new features, or promoting product (Security patches may still be provided).

End-of-Service (EOS) - Date product is no longer serviced via upgrades, patches, or maintenance.

Values for the “operatingSystem.lifecycle.stage” token include: EOL, EOL/EOS, GA, Not Applicable, Unknown

Values for the “software:(lifecycle.stage” token include: EOL, EOL/EOS, GA, Not Applicable, OS Dependent, Unknown

Software Lifecycle Search Tokens

Attribute	Examples	Search Token
lifecycle stage	"Beta", "GA", "EOL", "EOS"	software:(lifecycle.stage:
General Availability date	Apr-21-2014	software:(lifecycle.ga:
End-of-Life date	May-2016	software:(lifecycle.eol:
End-of-Support date	Jun-2018	software:(lifecycle.eos:

Qualys.

CSAM continuously tracks and curates data published by key software vendors to provide product lifecycle information in a standardized and structured format.

The slide lists the available search tokens in CSAM to identify software lifecycle information. Below is the explanation of the terminology used when referring to software lifecycle stages in CSAM:

GA (General Availability)

The software is in production, available for purchase, and supported

EOL (End of Sale)

No longer being sold by vendor

EOS (End of Support)

When it's no longer serviced via upgrades, patches, or maintenance

OS Lifecycle Search Tokens

Attribute	Examples	Search Token
Lifecycle state	"GA", "EOL", "EOS"	operatingSystem.lifecycle.stage
Support Stage	"Premier", "Extended", "Obsolete"	
General Availability date	Feb-15-2008	operatingSystem.lifecycle.ga
End-of-Life date	Nov-23-2013	operatingSystem.lifecycle.eol
End-of-Support date	Jun-18-2015	operatingSystem.lifecycle.eos

Qualys.

CSAM also tracks and curates data published by key OS vendors to provide OS lifecycle information in a standardized and structured format.

The slide lists the available search tokens in CSAM to identify OS lifecycle information. Below is the explanation of the terminology used when referring to OS lifecycle stages in CSAM:

GA (General Availability)

The OS is in production, available for purchase, and supported

EOL (End-of-Life)

No longer being sold or marketed by vendor

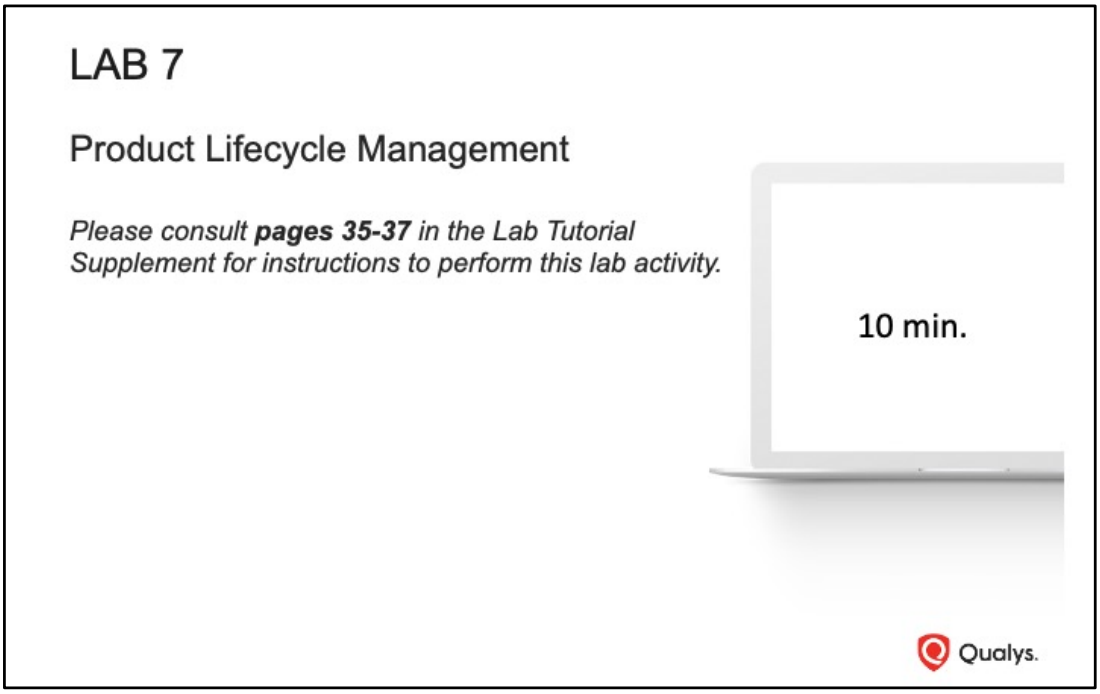
EOS (End-of-Support)

Refers to the date when it's no longer serviced via upgrades, patches, or maintenance

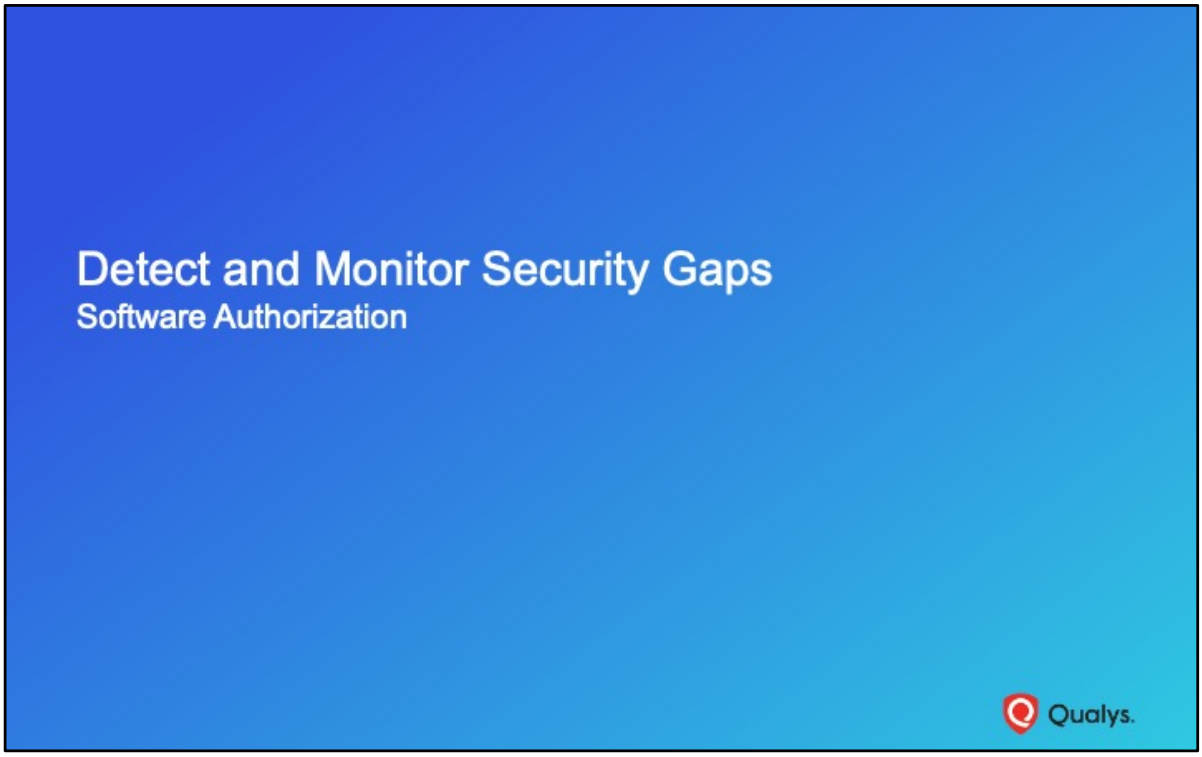
Additionally, what if you want to know about EOL that is *coming up*. You can search into the future and say, tell me my OS that is going to be EOL in the next 3 months, or 6 months, etc:

```
operatingSystem.lifecycle.eol: [now ... now+3M]
```

Note: Regarding lifecycles, CSAM has 10 to 20 times more lifecycle information than what you would find in QIDs.



Lab 7 will walk you through the steps to understand how CSAM provides vital information regarding product lifecycle stages.



This section helps you to define and create list of Authorized and Unauthorized software and track the result in your IT environment.

Proactive tracking of unauthorized and authorized software is a key tool to reduce security risks and improve the health of your assets. We often see customers driven by regulatory or other requirements that need them to have a security policy that defines authorized and unauthorized software lists and can implement such policies.

Center for Internet Security (CIS), Critical Security Control (CSC), Control 2 (CSC 2) is focused on the Inventory of Authorized and Unauthorized Software. It states that organizations must:
“Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution”.

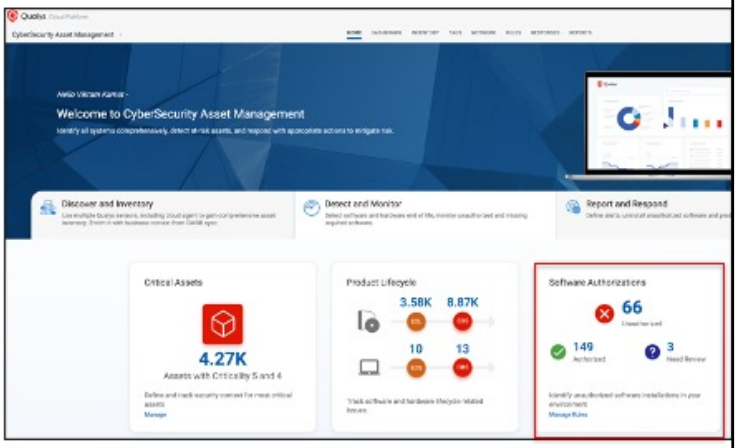
Organizations need an easy way to setup such a policy and operationalize it in their IT inventory.

CSAM allows you to define a set of software authorization rules and apply them to a selected set of assets.

Tracking Authorized & Unauthorized Software

Define, track, and alert installations of authorized/unauthorized software

- Define software rules for specific scope by asset tags
- Rules can include list of authorized and unauthorized software products, including software that needs review
- Identify and track assets with unauthorized software installations
- Establish structured alerts for at risk applications

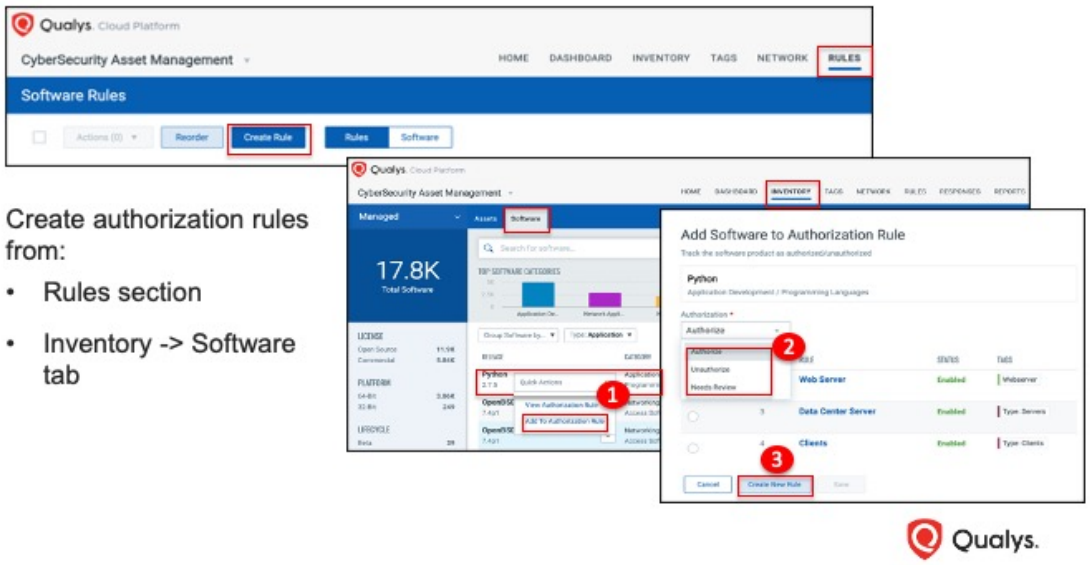


Qualys.

In CSAM, you can create rules to define software authorization (authorized, unauthorized, and needs review). Rules help you to track and report installations of authorized and unauthorized software based on user defined lists. For eg. your policy may state that there no web browser should be allowed on production database assets as a lot of vulnerabilities are identified on browsers.

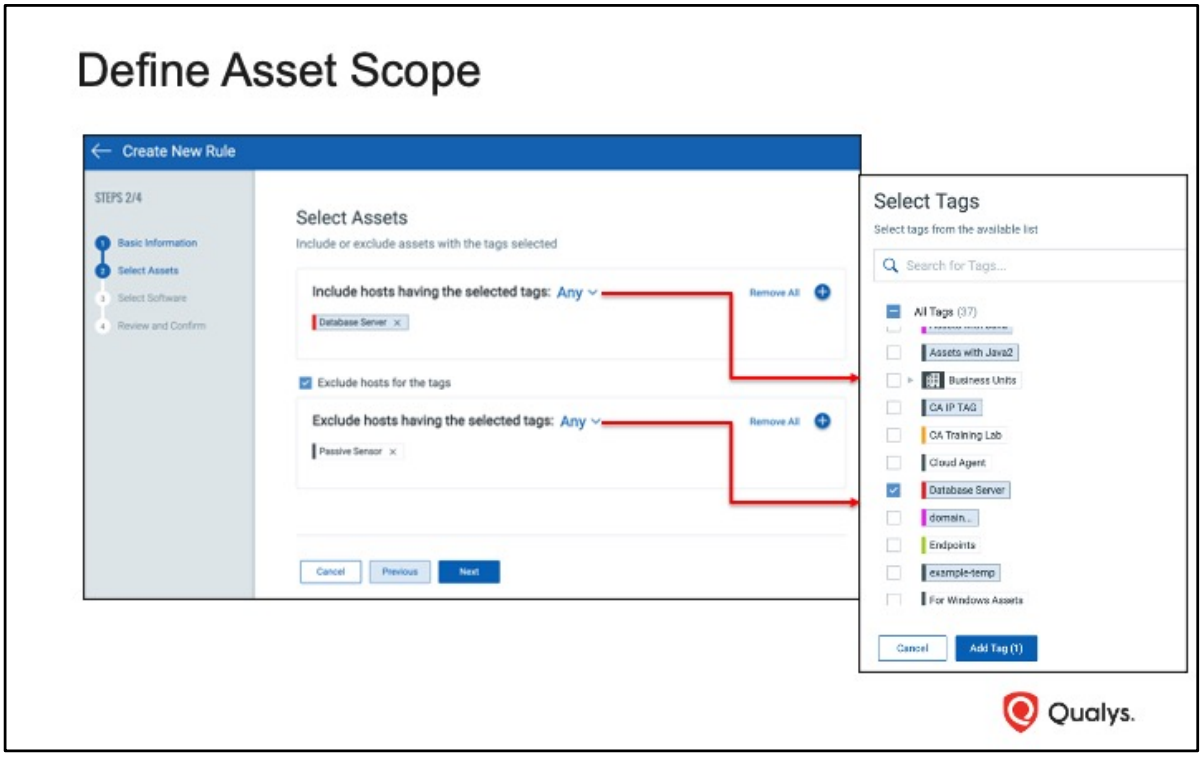
Once rules are created and evaluated, you can identify and track assets with unauthorized software in your environment. You can also set up rule-based alerts to notify users about asset health issues including software authorization requiring their attention.

Create Software Authorization Rules



You can create new authorization rules in two (2) ways:

- By going to Rules tab and creating new rule for software authorization.
- By selecting a quick action on the Inventory->Software tab on the title you want to create the rule for.

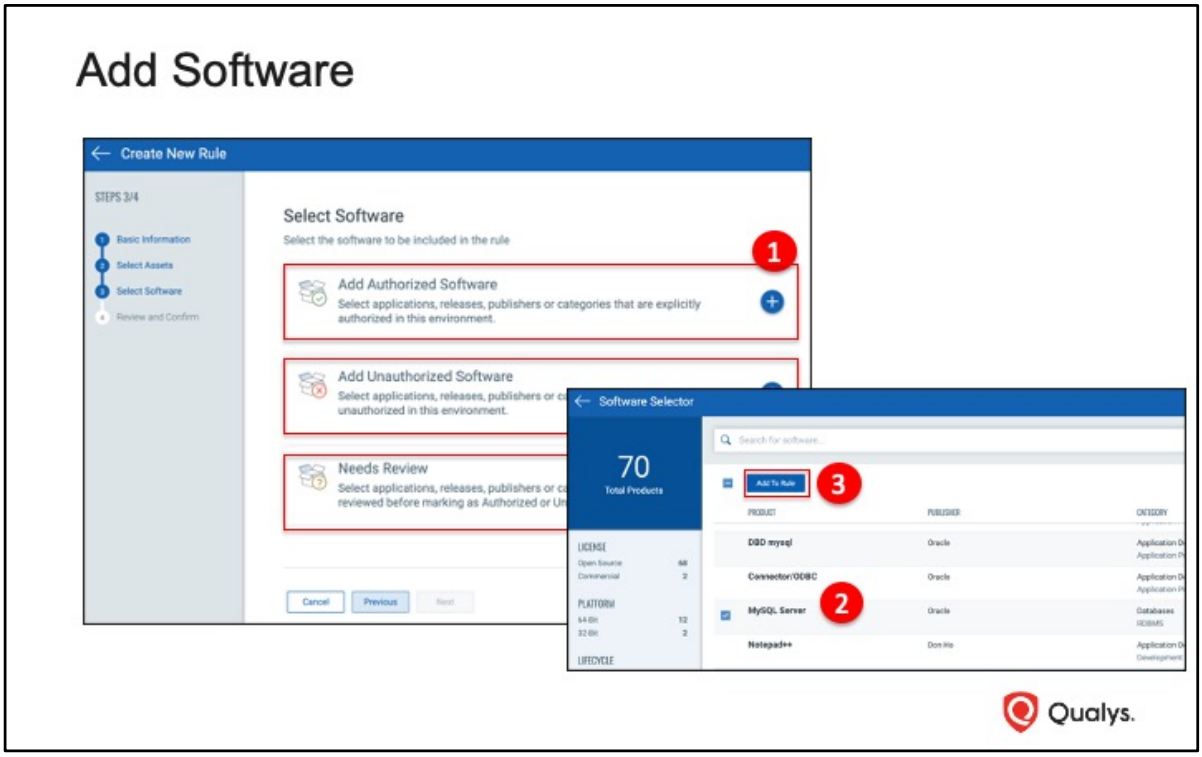


You may need to implement different authorization rules in different parts of your environment. For instance, Firefox may be authorized on workstations and laptops but not on server assets.
Asset Tags make it easy to include or exclude specific assets within the rule scope.

In the Select Assets step, you can select tags to include and exclude the assets in the rule which helps you define the scope of the authorization (e.g. Firefox browser is authorized on personal computing devices, but unauthorized on server devices).

Note: For the newly created asset, software authorization rule won't be applied to the asset because tag evaluation happens after the asset creation. In subsequent scan, the software authorization rule will be applied to the asset.

Add Software

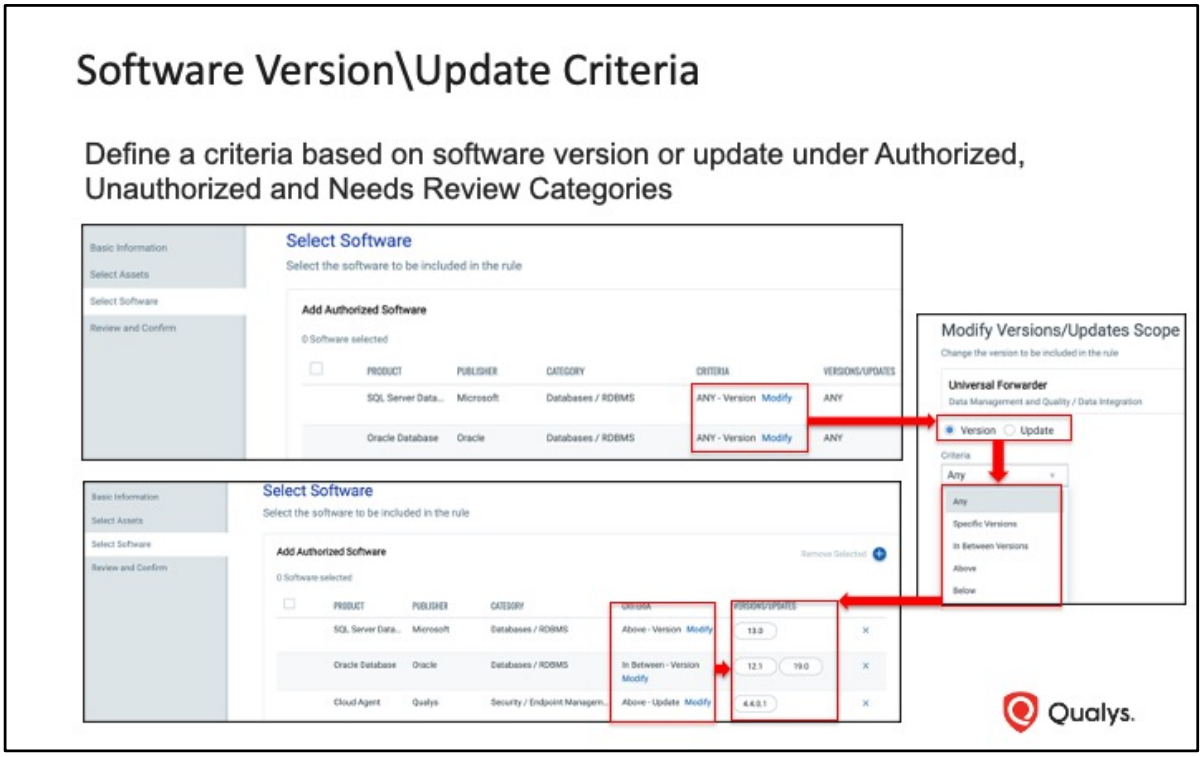


In the Select Software step, add and select Authorized Software, Unauthorized Software, and software that Needs Review to be included in the rule.

When you click the plus (+) sign under any of the categories to select software, the Software Selector window comes up where you can search and select the software with software name.

Note that the software inventory data listed here comes from authenticated scans from a scanner appliance or from Cloud Agent scans of assets associated with the selected Asset Tag(s).

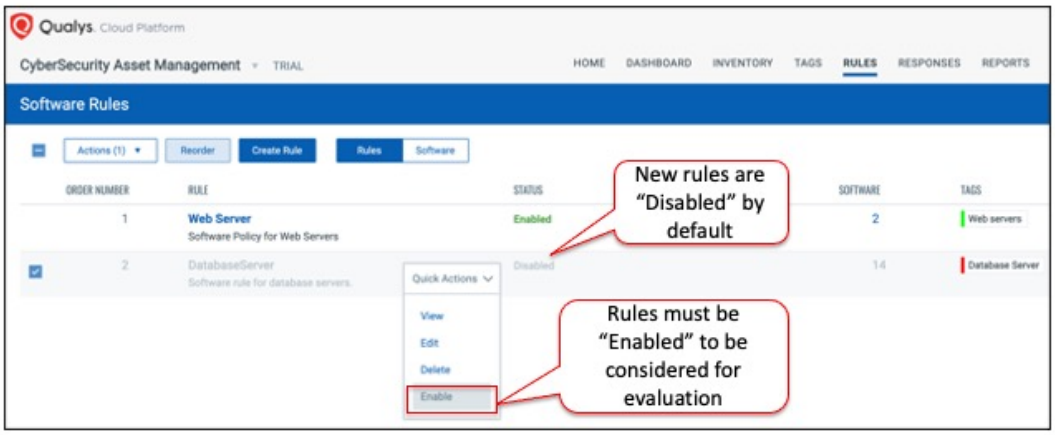
Select the software and click **Add To Rule**.



Once you add software to the Authorized, Unauthorized, and Needs Review categories, you can **Modify** the default “ANY – Version” criteria to select appropriate software versions or updates for the rule.
You can select software with different versions and/or update criteria from the following list:

- ANY
- Specific
- In Between
- Above
- Below

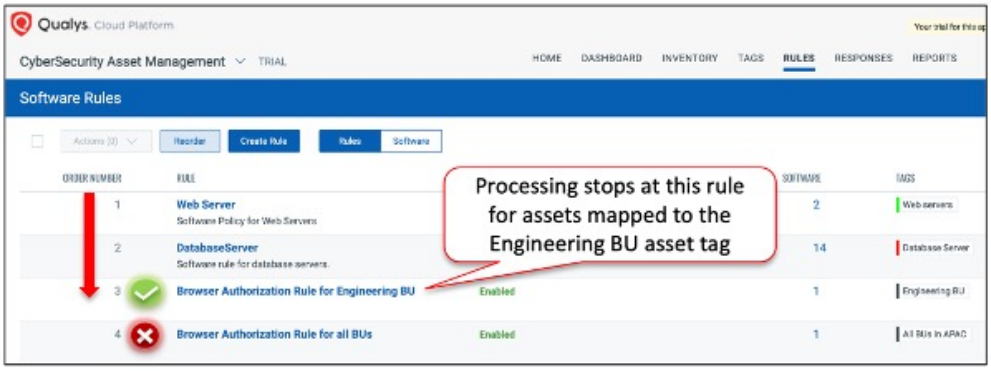
Rule Status



Qualys.

By default, any new rule is set to the Disabled status. This is just so that you can review and reorder the rule as required, before it is applied to your environment. You can reorder the rule to define the priority of the rule before enabling it.

Rule Order



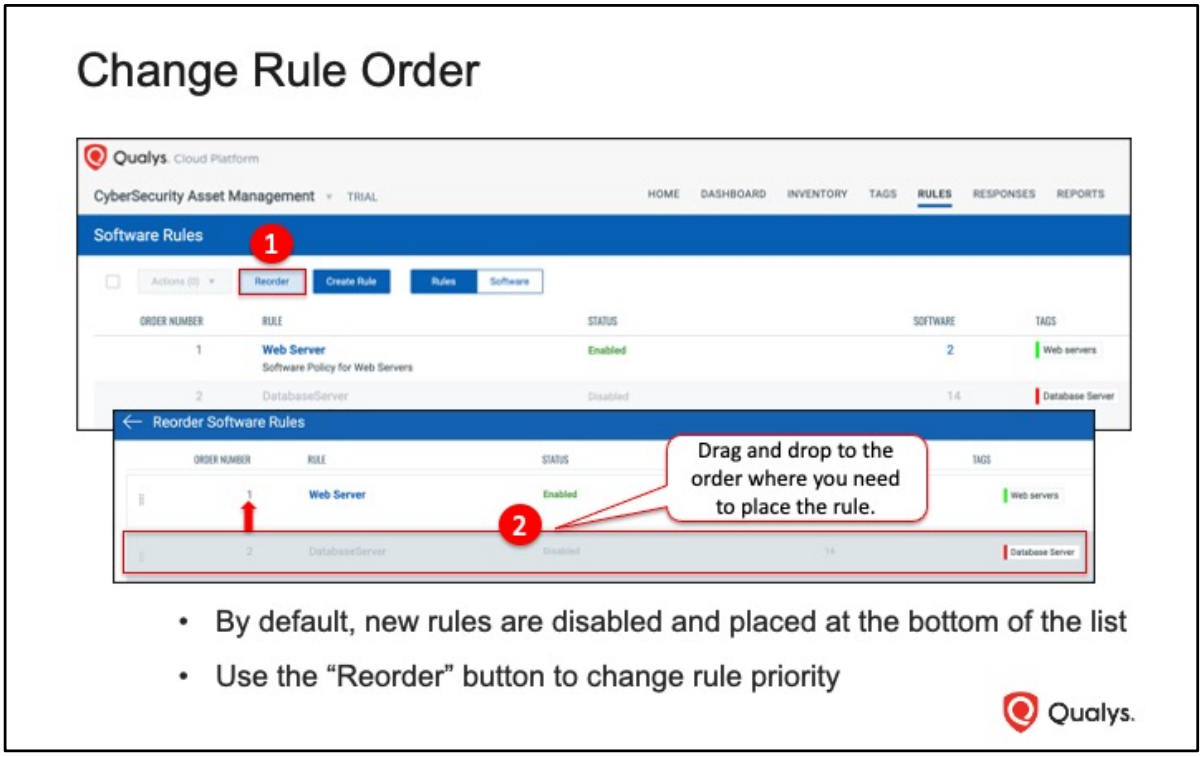
- Rules are processed from top to bottom in their priority order
- Rules with higher priority are placed at the top of the list and take precedence
- When there is a rule match for a software for an asset, no subsequent rules are applied on it
- Place rules with a global scope towards the bottom of the list

Qualys.

Rules with higher priority take precedence over rules with the lower priority. Rules with higher priority are placed at the top of the list.

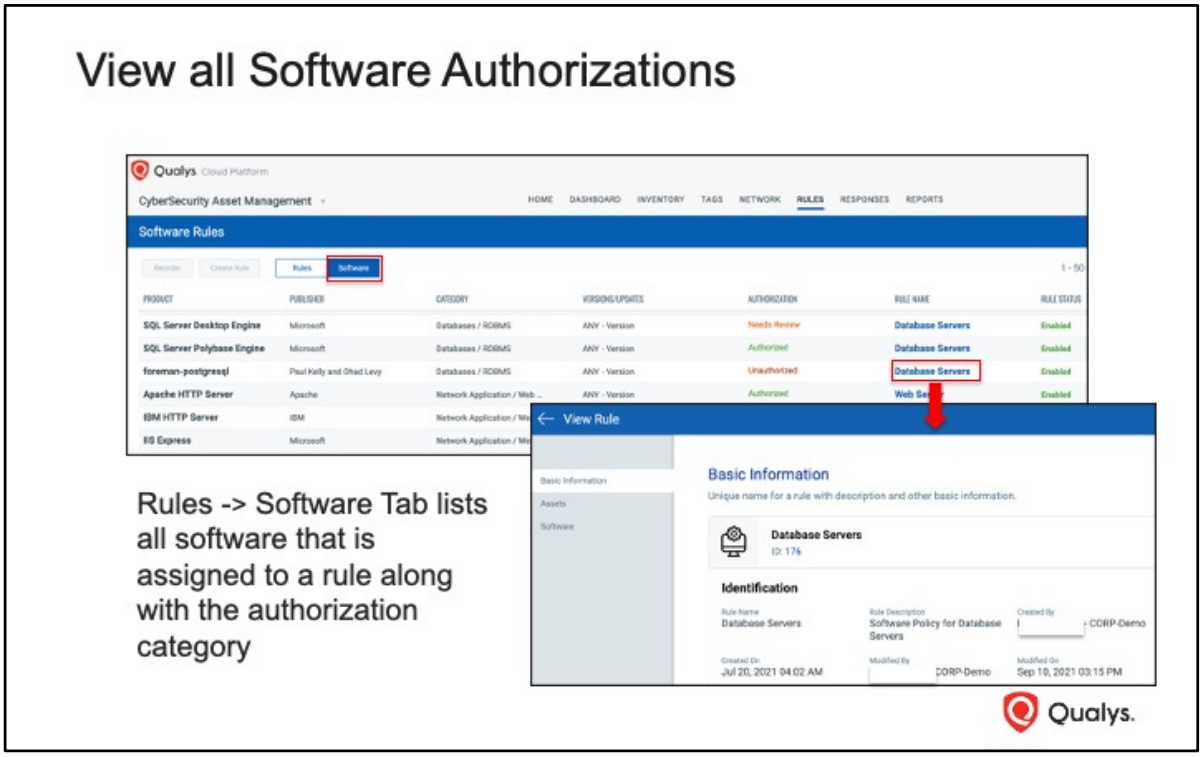
If a software is included in the multiple rules, then reordering the rule plays vital role and decides priority while taking effect. For example, you could unauthorize Firefox on all devices, then authorize Firefox for use by the engineering team on their devices. In this case, you will need to place global unauthorization rule below authorization rule for the engineering team.

In this illustration, the “Engineering BU” is a child tag under “All BUs in APAC” and the software being evaluated is the Firefox browser.



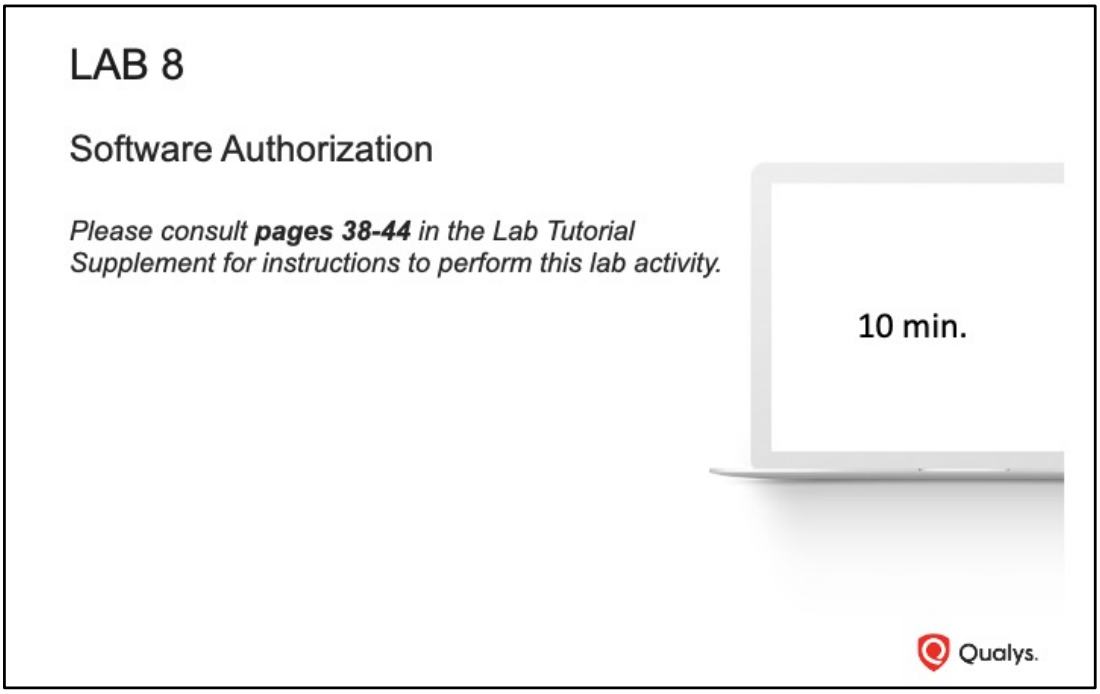
By default, any newly created rule is placed at the bottom of the list. To reorder the rule, select the rule and click **Reorder**.

You can simply drag and drop the rules to reorder their priority. Make sure your rule is with Enabled status to take effect.

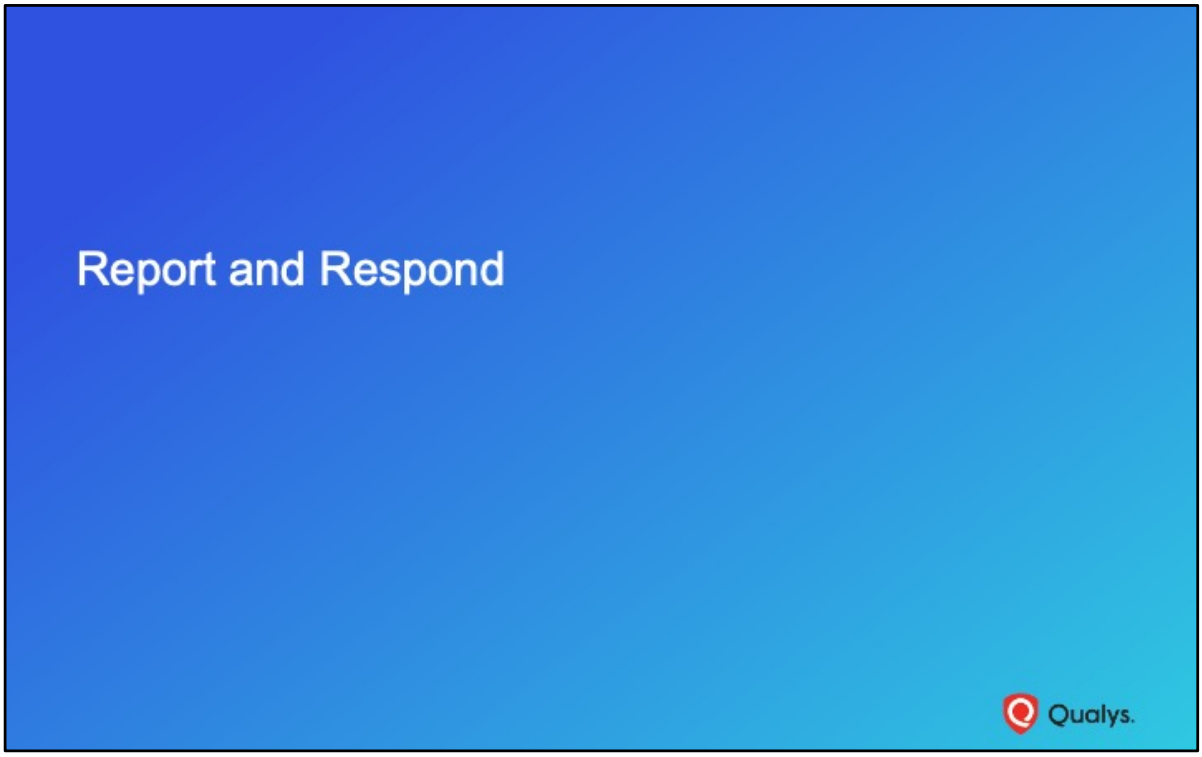


Under the RULES section, **Software** tab you can view the list of all software with publisher, category, version/update, authorization status, software authorization rule mapped to the software and rule status.

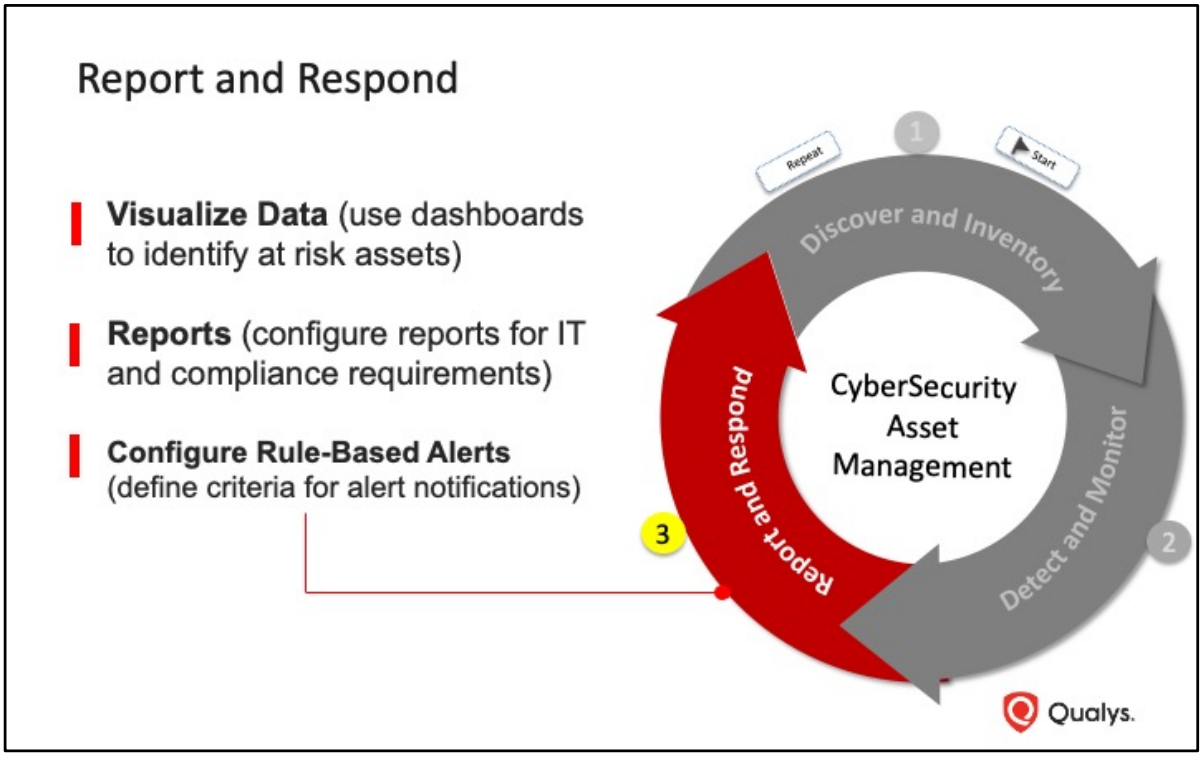
Clicking on the rule shows basic information about the rule, the assets in scope and the Authorized/Unauthorized/Under Review software list configured within the rule.



Lab 8 will walk you through the steps to configure rules for software authorization in your Qualys account.

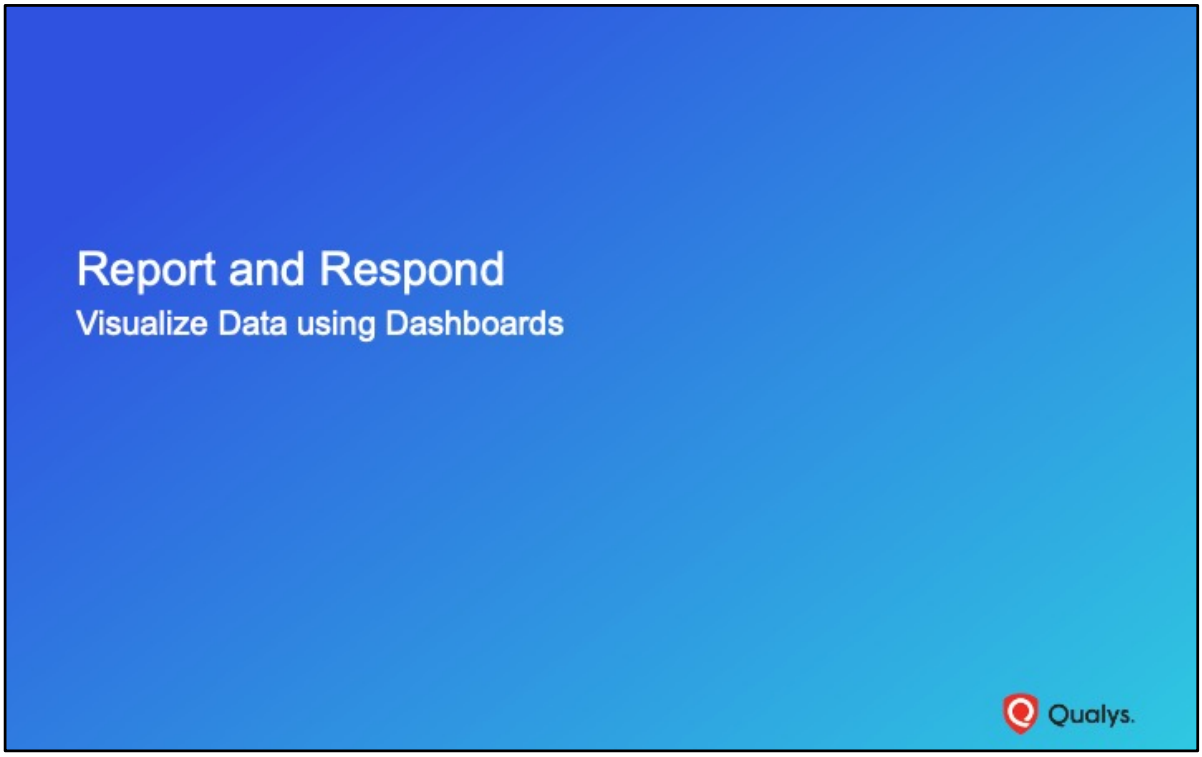


This section covers how to visualize asset data using dashboards, configure reports and setup rule-based alerts to notify interested parties of at-risk assets.

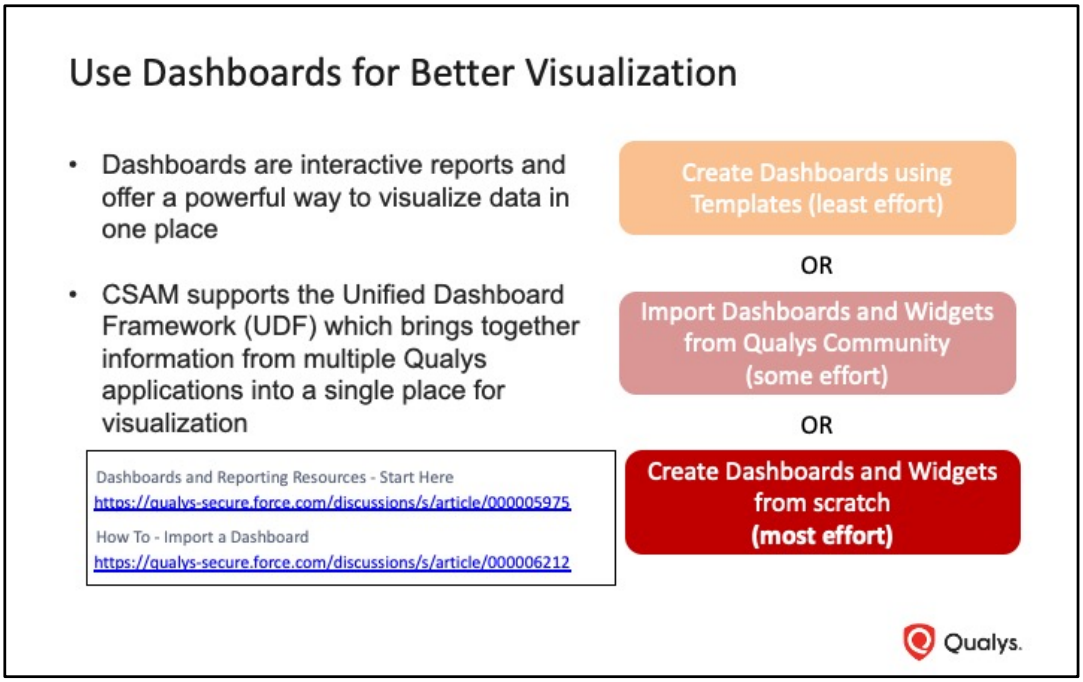


Report and Respond

The final step (step 3) involves using reports (using templates and dashboards) to keep track of all asset inventory and using rule-based asserts to notify you of critical events such as unauthorized software installations, low disk space events, etc.



This topic focusses on using dashboards to easily and quickly see what parts of your environment that are at risk.



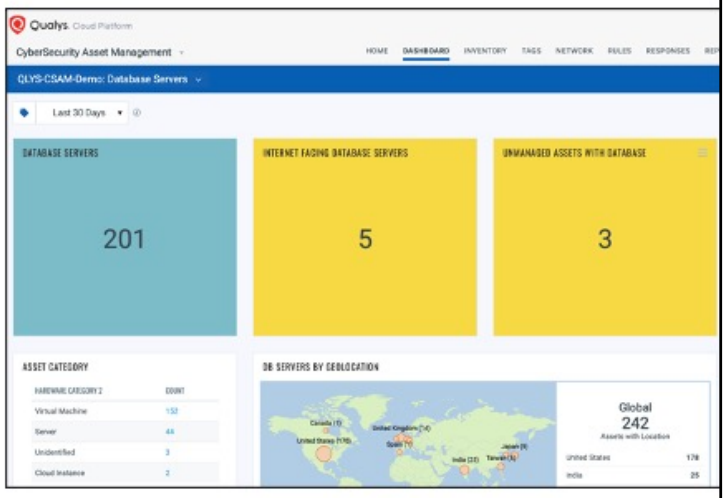
Queries, widgets and dashboards can be used across multiple apps in Qualys, including in CSAM. These reporting tools help you get the required data fast.

CSAM supports the Unified Dashboard Framework (UDF) which brings information from all Qualys applications into a single place for visualization. UD provides a powerful new dashboarding framework along with platform service that will be consumed and used by all other products to enhance the existing dashboard capabilities. You can use widget builder and improvise dashboards to make it uniform across all products.

You can create your own dashboard using existing widget templates that we provide, customize existing widgets or create your own widgets to suit your need.

Track Database Instances and Security Gaps

- Discover, Inventory & Categorize Databases with criticality
- Identify unmanaged Database server assets
- Track & Manage Unauthorized database software policies
- Manage Database lifecycle for EOL, EOS
- Apply key business data from CMDB to gain additional context



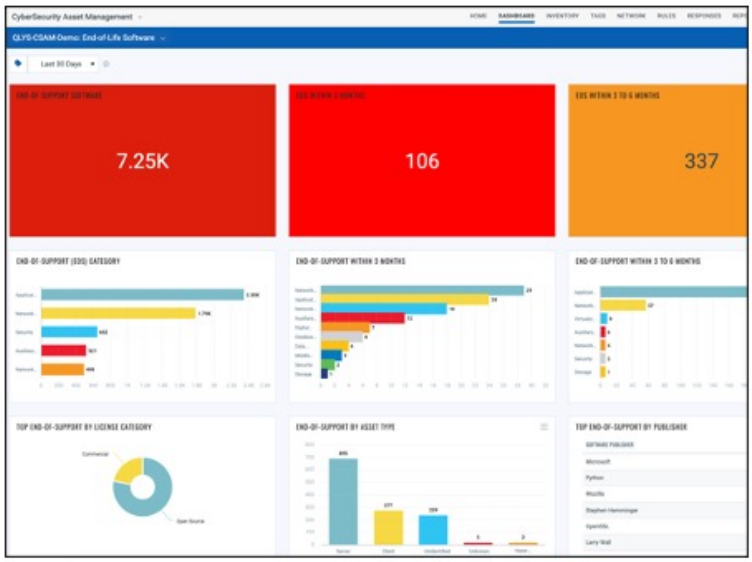
Qualys.

Using dashboards you can get a better visualization of your overall database inventory and track their security gaps.
You can use dashboard widgets to

- Discover and organize your database apps and instances
- Identify unmanaged database server assets
- Identify internet exposed database servers
- Track and manage unauthorized database instances using security policies
- Track and manage database software lifecycle
- Use business information synchronized from ServiceNow CMDB sync (support group info, business apps with database servers,etc.) to apply business context and prioritize remediation of critical assets
- And more..

Reduce Risk by Managing Software Lifecycle

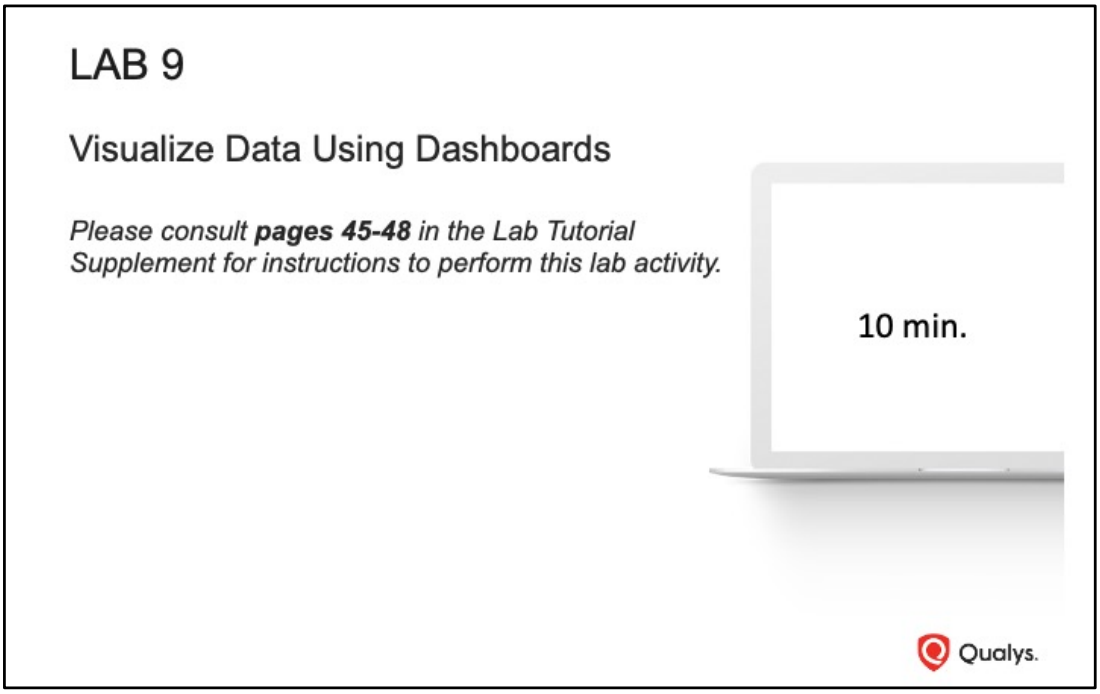
- Looking at individual assets or software for lifecycle information is time consuming
- Use dashboards to quickly see parts of your environment that are at risk
- Know about upcoming lifecycle events to plan ahead of time



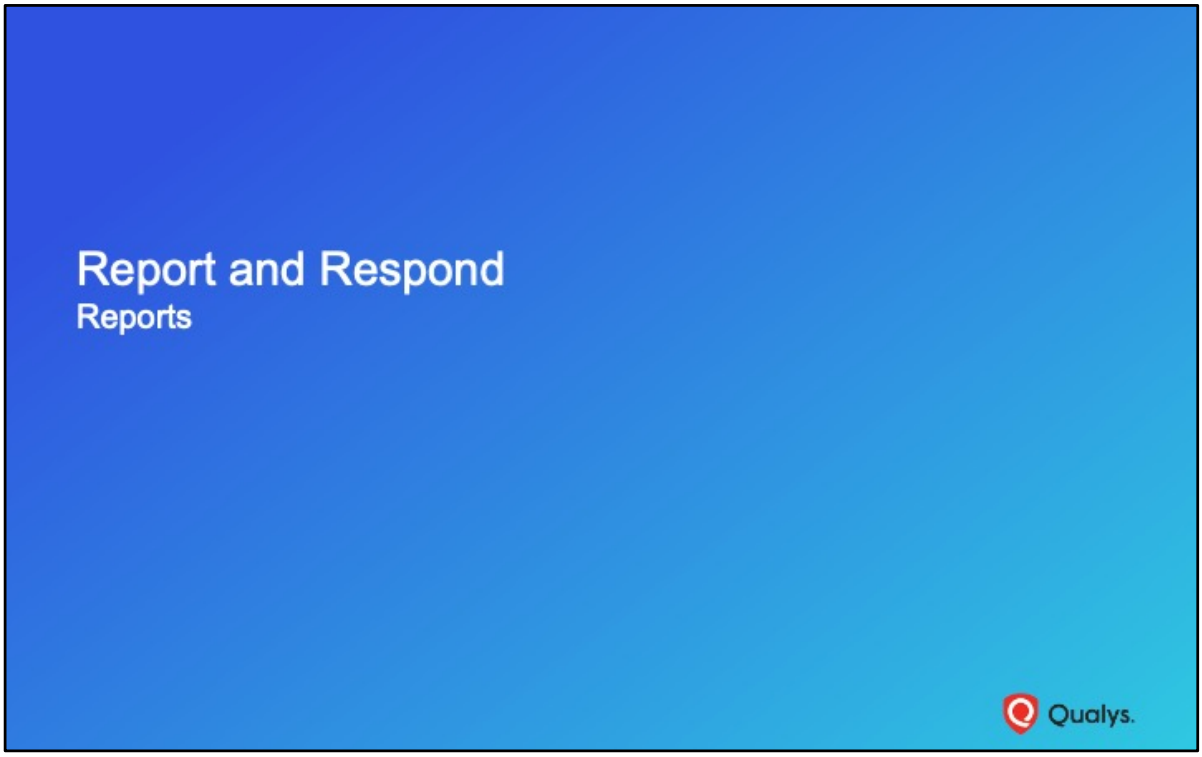
Qualys.

End of Support (EOS) software is no longer actively managed or patched by vendors. Over time, such software becomes more and more susceptible to vulnerabilities because the attack surface is no longer a moving target. This creates opportunities for attack scripts that can be distributes to less skilled attackers who do not have to understand how they work in order to use them. And it is important for organizations to know ahead of time about software getting EOL or EOS since it takes months of planning to address. We hear all the time about situations where organizations realize a software product is going EOS a month or two beforehand and then they have to really scramble to upgrade or remove such software, causing huge upheaval in their business.

You need to be able to easily and quickly see what parts of your environment are at risk. You don't have time to look at each individual assets or software products. That's where visualization through dashboards come into play.

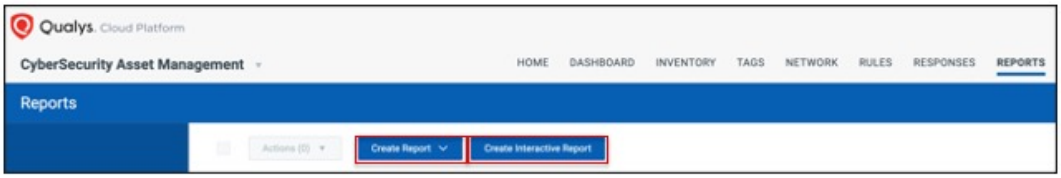


Lab 9 will walk you through the steps of using dashboards for visualization of key asset and security data in your Qualys account.



This section provides an overview of steps to build customized reports for tracking asset and software inventory, compliance and security gaps.

Reporting



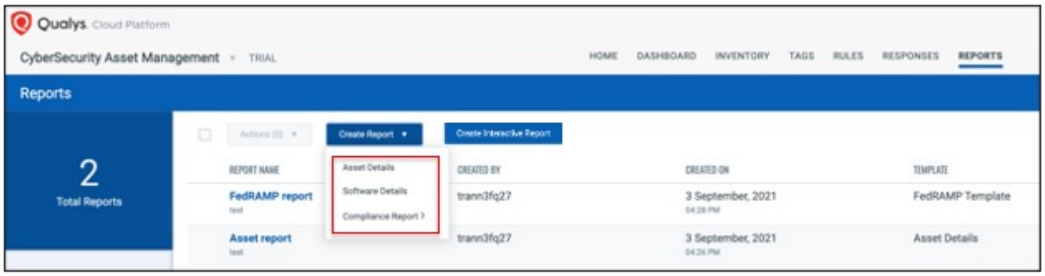
- Generate reports to meet industry and standards compliance needs
- 2 types of reports are available:
  - **Asset**, **Software** and **Compliance reports** - Focussed on inventory Data
  - **Interactive Report (Beta Feature)** – Focussed on identifying security gaps (Obsolete hardware, EOL/EOS software, unauthorized software, etc.)

Qualys.

CSAM allows you to create customized reports for asset, software, and compliance (currently includes a FedRAMP template). These reports are focussed on inventory data.
In addition, CSAM also provides an interactive workflow that helps users identify and list security gaps across a set of assets of given asset tag(s).

Custom Inventory and Compliance Reports

Generate reports to meet industry and standard compliance needs.



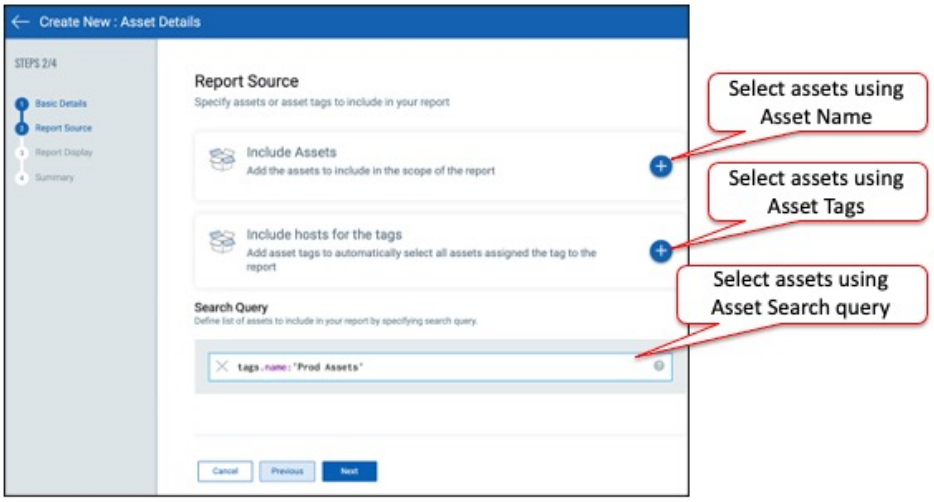
- Create custom CSV reports
  - Define asset scope and filter attributes for the report
- Select out of the box report templates:
  - Asset Details *(host information)*
  - Software Details *(host and software information)*
  - FedRAMP Compliance *(host and software information as required by RedRAMP)*

Qualys.

You can create three types of reports:

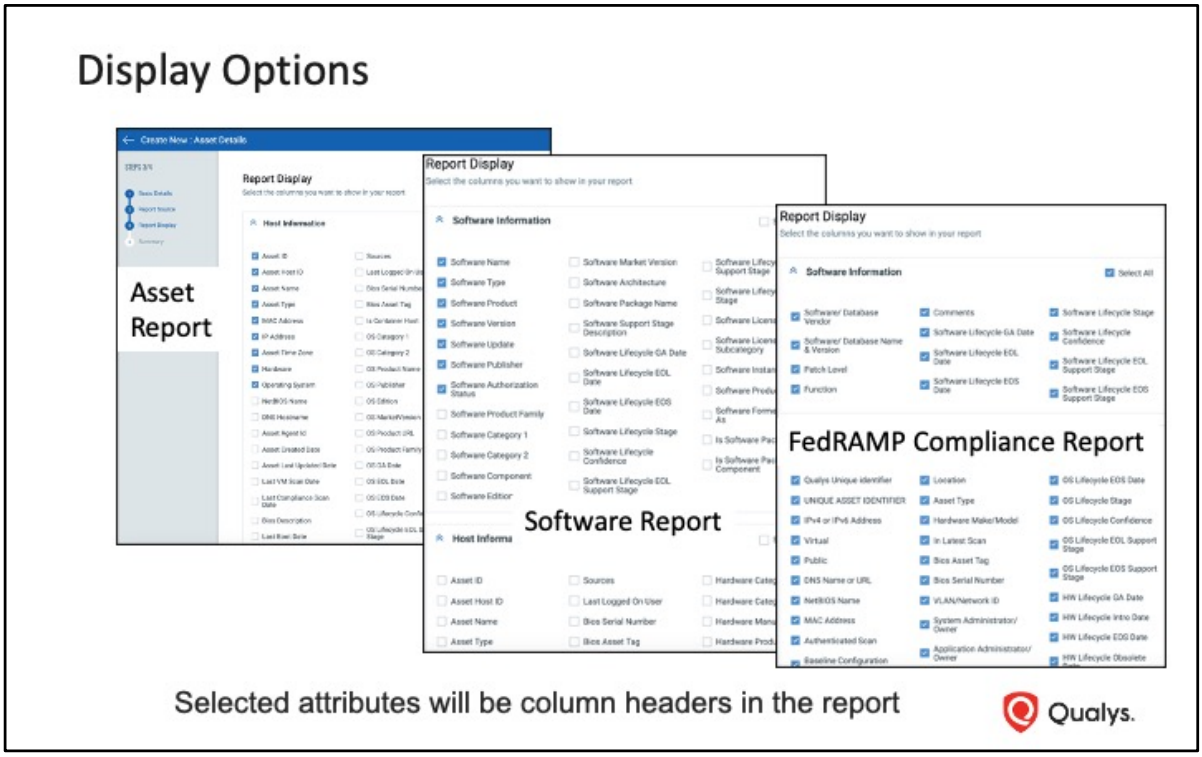
- Asset Details - shows detailed report of the selected assets based on host information (attributes).
- Software Details - shows detailed report of the selected assets based on software and host information (attributes).
- Compliance Report - shows detailed report of the assets for FedRAMP compliance based on software and host information (attributes)

Report Source



Qualys.

In the Report Source step, you can define the scope of the assets to be included in the report. You can select assets with asset name, asset tag, or using search query.

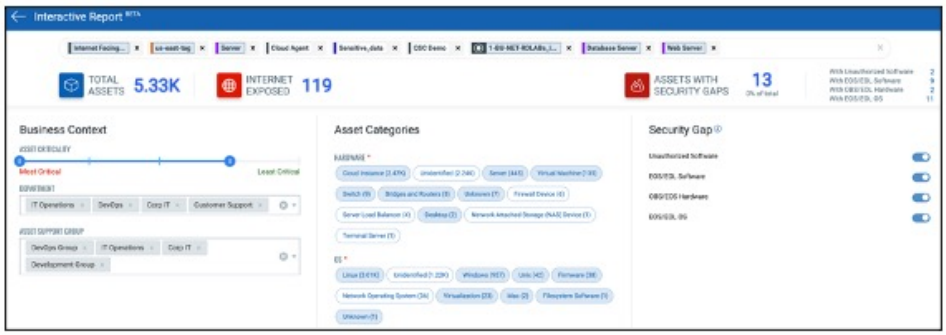


In the Report Display step, select host and software attributes to be included in the report. The selected attributes will be column headers in the report..

For Asset Report, only Host Information fields apply. For Software and FedRAMP Compliance report, both Software and Host Information fields are available for selection.

The Host and Software information fields available in the FedRAMP compliance report are as per FedRAMP requirements.

Interactive Report



- Includes an interactive workflow to identify and list security gaps across a set of assets of given asset tag(s)
- Focusses on issues rather than inventory

Note that the Interactive Report feature is currently in Beta release. Please contact your Qualys TAM to enable it for your account.

Qualys.

Salient features of Interactive Report:

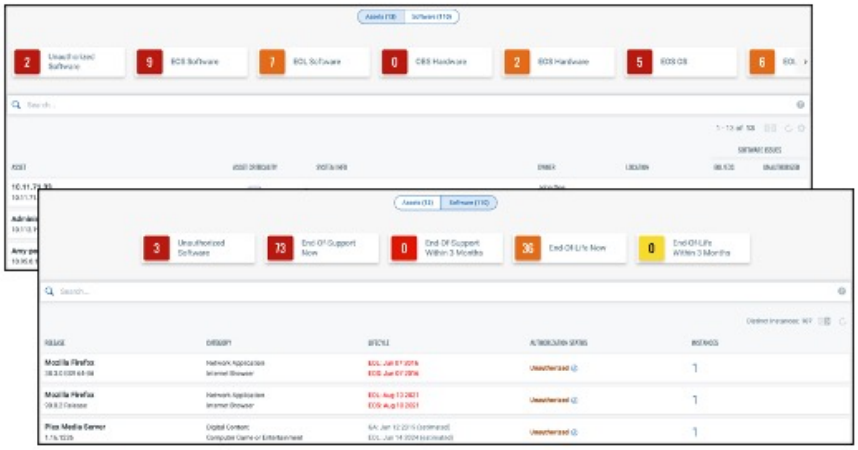
- Similar to the VMDR Prioritization report, the interactive report provides an interactive workflow that helps users identify and list security gaps across a set of assets of given asset tag(s).
- It focuses on issues, rather that entire inventory.
- Allows users to quickly understand the types of issues that can be highlighted and helps users quickly narrow down the issues with interactive filters.

Upcoming enhancements:

- Allows users to save these views for later access.
- Allows users to share information via summarized dashboards with key metrics as well as detailed reports via csv exports.

Please contact your Qualys TAM for more information.

View Asset-Centric or Software-Centric Results



Allows report users to view list of assets or software matching the security gap criteria

Qualys.

Asset-Centric Results

As a report user, you can view the list of assets that match ANY (or multiple) of the "Security Gaps" you configured for review in the Interactive Report.

Just below the "Assets" tab, you can see a summary of counts of issues:

- Unmanaged Assets
- EOL/EOS Hardware
- Unauthorized Software
- EOL/EOS Software
- EOS OS

Clicking on these cards/numbers filters assets as per the identified security gap.

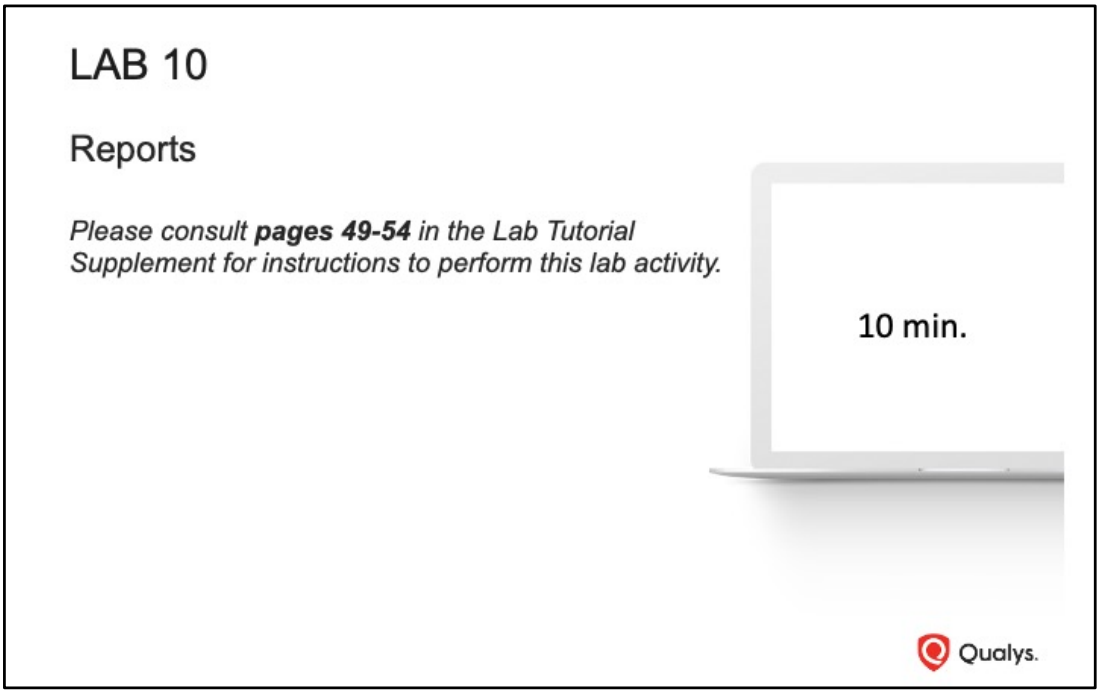
Software-Centric Results

As a report user, you can view the list of software that match ANY (or multiple) of the "Software Security Gaps" you configured for review in the Interactive Report.

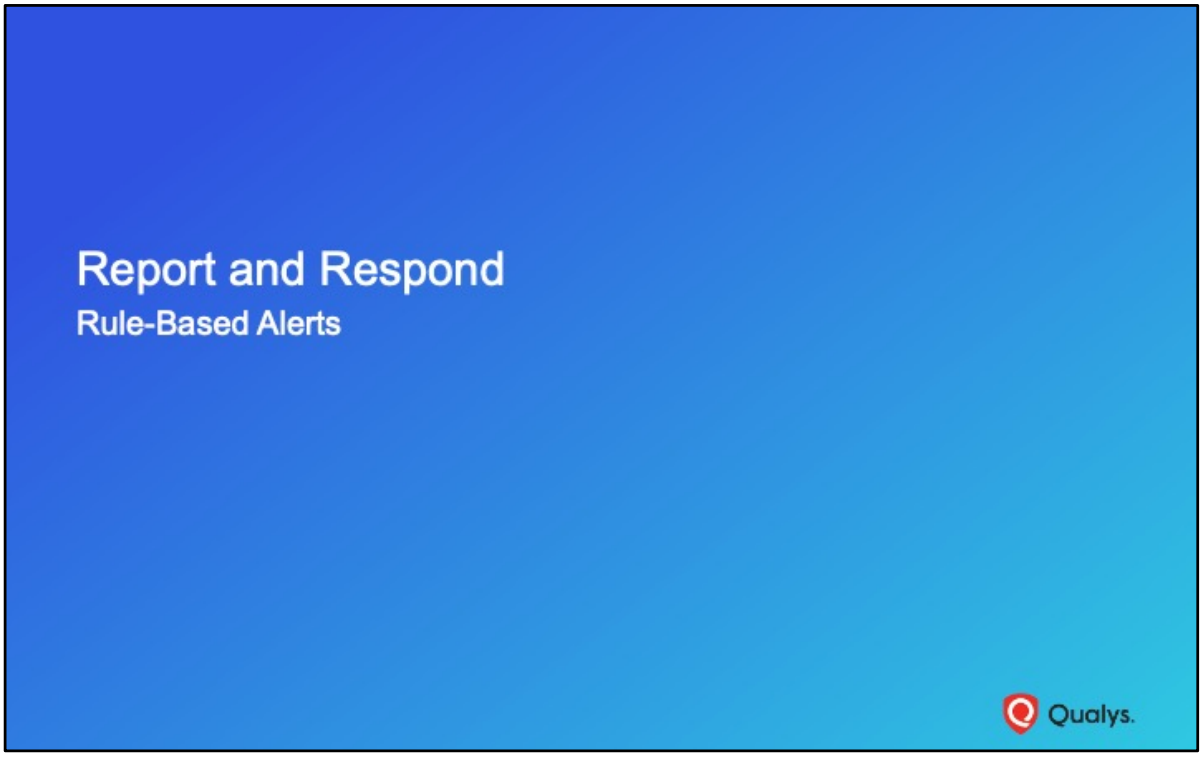
Below the "Software" tab, there is a summary of counts of issues:

- Unauthorized Software
- End-of-Support Now
- End-of-Support Within 3 Months
- End-of-Life Now
- End-of-Life Within 3 Months

Clicking on these cards/numbers filters the corresponding Software Releases.



Lab 10 will walk you through the steps to generate interactive and on-demand reports in your Qualys account.

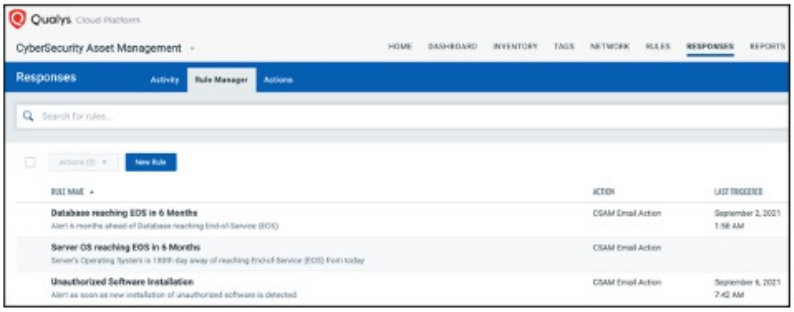


This section covers rule-based alert configuration to notify users about asset health issues requiring their attention.

Alerting

Immediately notify your teams of important security gaps impacting the overall health and security hygiene of critical assets.

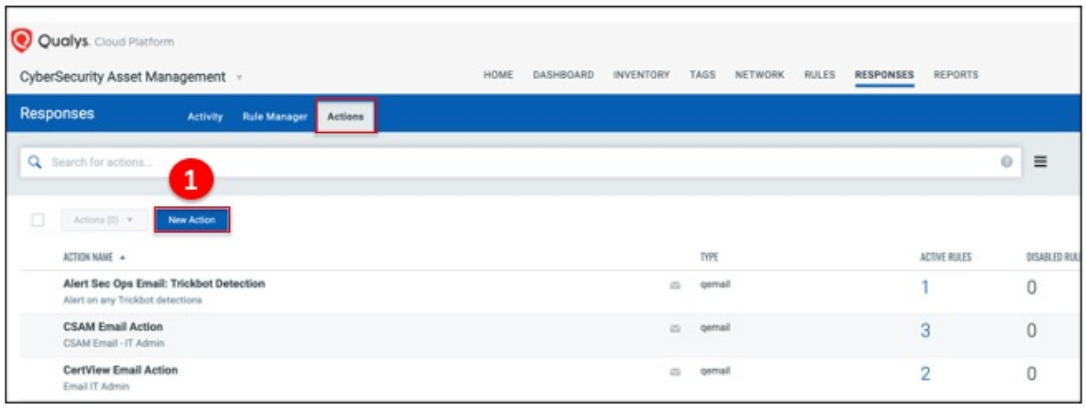
- Rule/QQL driven alerts
- Out-of-box templates/examples
- Notification via Email, Slack & PagerDuty



Qualys.

In order to effectively manage your inventory, you should setup Responses (notifications) to alert you about conditions requiring attention (e.g. hardware or software end of life events, installations of unauthorized software, etc.).
You can configure rules to monitor critical events that satisfy the conditions specified in a rule and send you alert messages if events/incidents matching the condition are detected. The alert message will have the event details.

Configure New Action



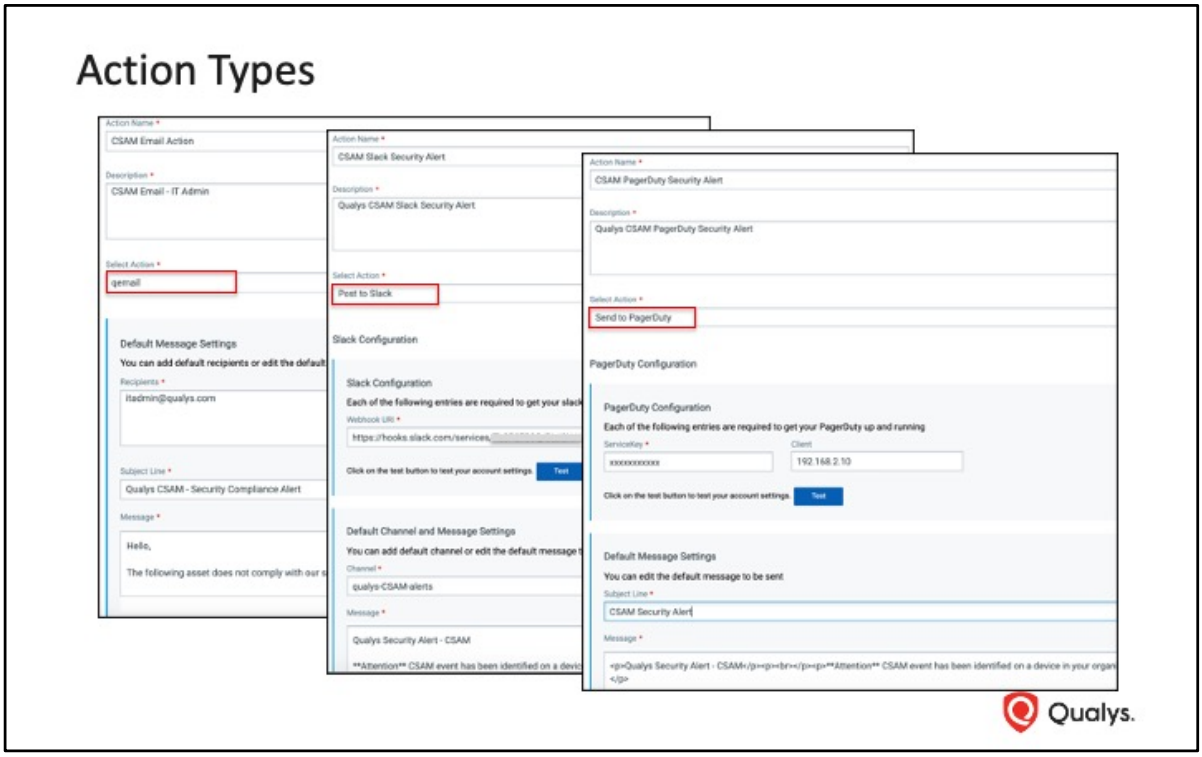
Step 1: Configure a rule action that will be referenced in the alert rule

Qualys.

The first step is to configure a rule action that will be referenced in the alert rule. You can configure a rule action under the Actions tab in the Response section.

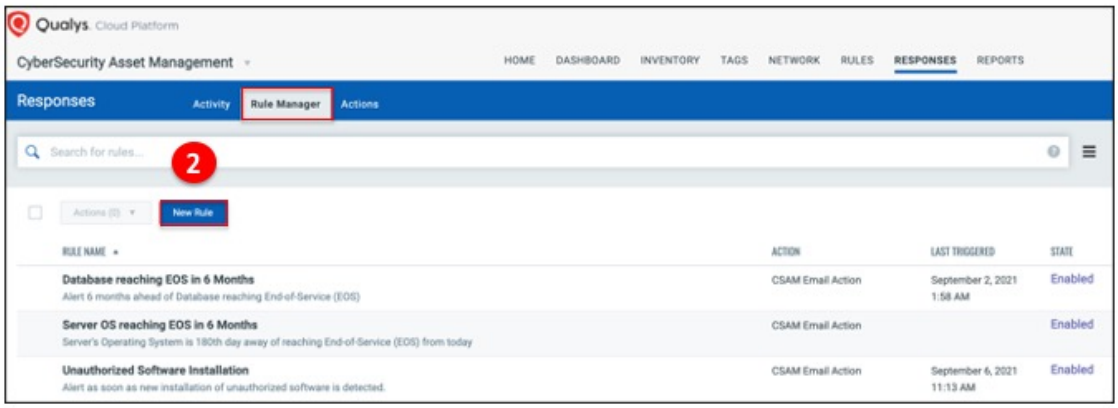
Provide a name and a description for the action and select an action from the Select Action drop-down.

Provide the settings for configuring the messaging system that Qualys will use to send alerts.



CSAM supports three (3) mechanisms for alerting:
- Select Send Email (Via Qualys) to receive email alerts. Specify the recipients' email ID who will receive the alerts, subject of the alert message and the customized alert message. Note that based on the configuration settings you will see either of the two options.
- Select "Send to PagerDuty" to send alerts to your PagerDuty account. Provide the service key that CSAM will require to connect to your PagerDuty account. In Default Message Settings, specify the subject and the customized alert message.
- Select "Post to Slack" to post alert messages to your Slack account. Provide the Webhook URI that CSAM will use to connect to your slack account to post alert messages. In Default Message Settings, specify the subject of the alert message and the customized alert message.

Configure New Rule

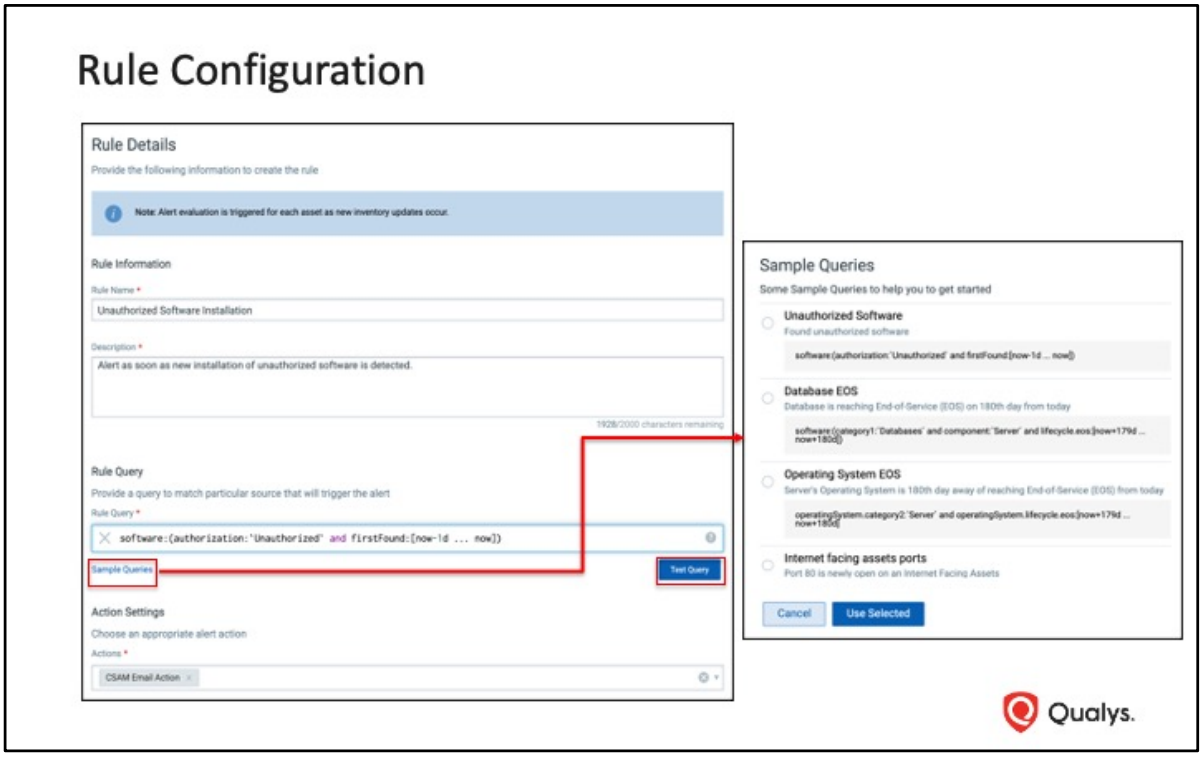


Step 2: Configure a rule specifying events you want to monitor, criteria for triggering the rule and actions to be taken on those events.

Qualys.

The next step is to configure a rule to generate alerts for critical events. You can configure rules under the Rule Manager tab in the Response section.

When a rule is triggered based on a condition match, CSAM will send you alerts using the configured action type that will have details of the events.

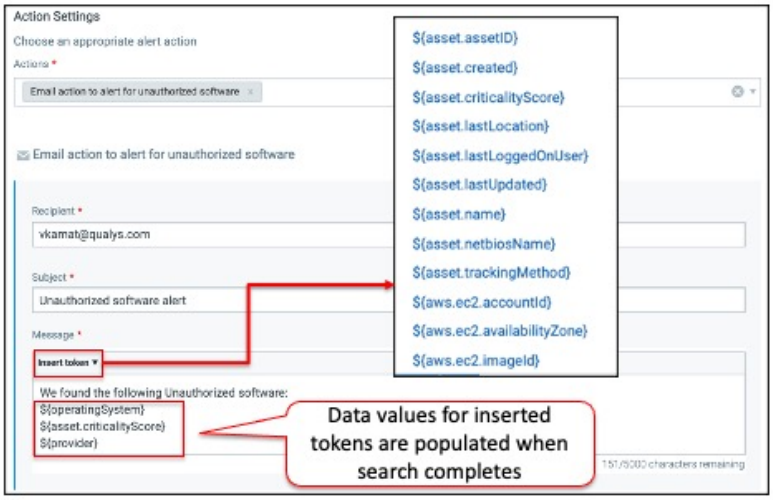


Provide required details in the respective sections to create a new rule:

- In the **Rule Information** section, provide a name and description of the new rule in the Rule Name and Description
- In the **Rule Query** section, specify a query for the rule. The system uses this query to search for events. The query illustrated in the slide looks for all unauthorized software installations detected in the last one day. Use the **Test Query** button to test your query. This will indicate if there are any events matching the defined criteria currently present in the environment.
- Click **Sample Queries link** to select from predefined queries. These queries cover product lifecycle, software authorization or other items such as open ports or insufficient server storage for alerting.

Insert Tokens

- Insert tokens in the message body to include relevant asset information in the alert
- Supported for all action types (Email, Slack, PagerDuty)
- Only tokens that help in asset scoping or those that are directly related to the alert evaluation are supported



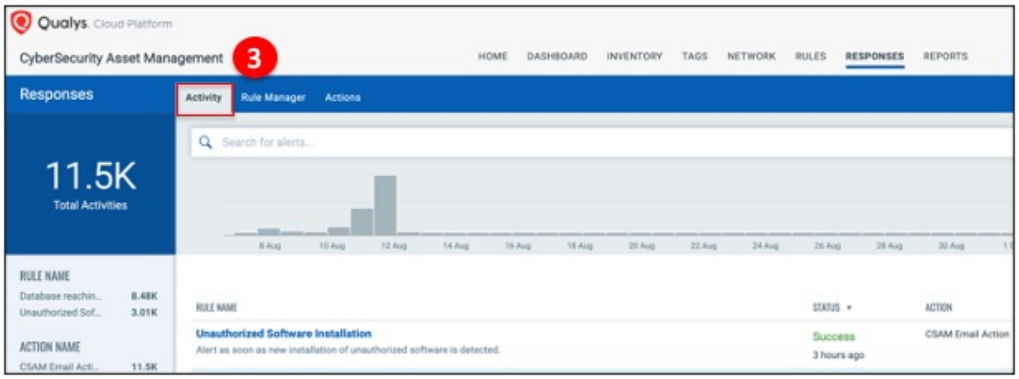
The Recipient, Subject and Message are automatically populated within the rule based on the selected Actions type.

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

Note that only tokens that help in asset scoping or those that are directly related to the alert evaluation are supported for alert rule creation. For instance, an AWS/Azure/GCP search token is only applicable if you have the relevant cloud connector configured in your Qualys account.

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

Manage Alerts



Step 3: Monitor all the alerts that were sent after the rules were triggered

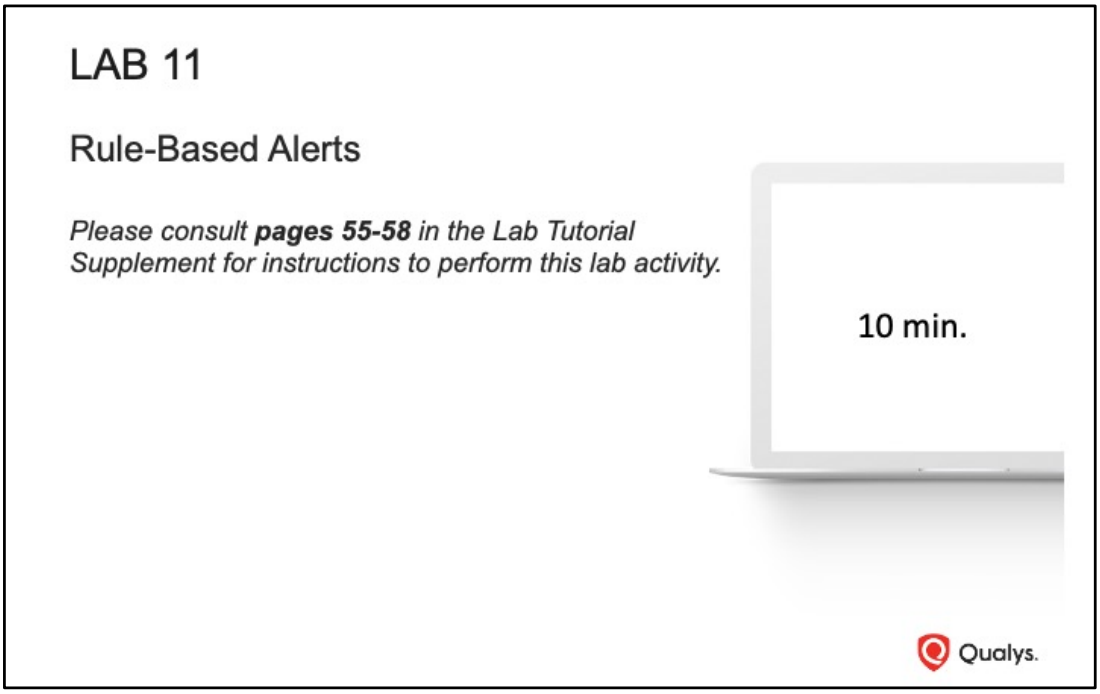
Qualys.

Step 3 - Monitor all the alerts that were sent after the rules were triggered.

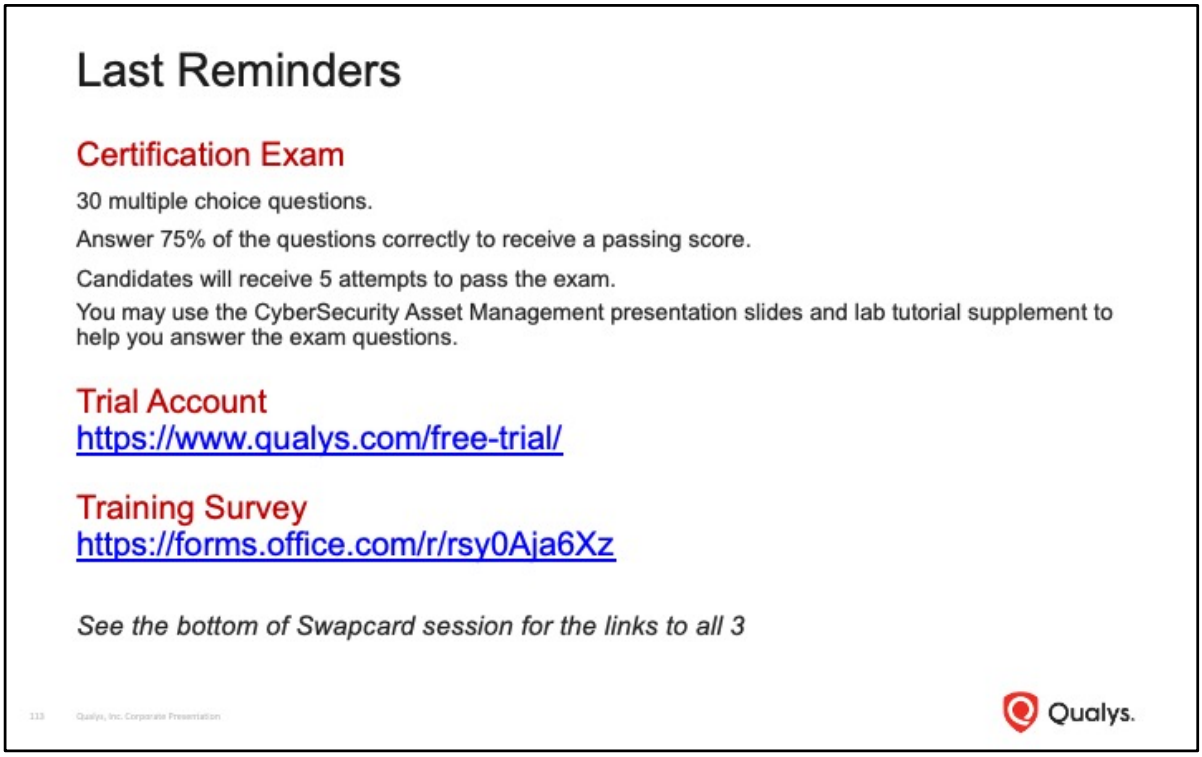
The Activity tab lists all the alert activity for the selected timeframe. Here you will see for each alert, rule name, success or failure in sending the alert message, action chosen for the rule, matches found for the rule and the user who created the rule.

Here you can search for alerts using our search tokens, select a period to view the rules triggered during that time frame, click any bar to jump to the alerts triggered in a certain timeframe and use these filters to group the alerts by rule name, action name, email recipients and status.

That's it! You are all set to start being alerted about your detections.



Lab 11 will walk you through the steps to configure rule-based alerts to notify users about asset health issues requiring their attention.



The link to enrol for the course and the certification exam is https://gm1.geolearning.com/geonext/qualys/scheduledclassdetails4enroll.geo?&id=22511237813

Please consult the Lab Tutorial Supplement for information regarding registration for the CyberSecurity Asset Management course certification exam.
NOTE: We recommend that you take this certification exam at the earliest possible convenience.

You can request a free Qualys limited trial account by submitting a request on this link https://www.qualys.com/free-trial/


Qualys
Thank You
training@qualys.com