



Qualys Global AssetView CyberSecurity Asset Management

Quick Start Guide

January 10, 2022

Table of Contents

Table of Contents	2
Introduction	3
Capabilities	4
Unlimited, continuous discovery	5
Normalization & categorization	5
Detailed asset information	6
Powerful Search	6
Create asset tags and define asset criticality	7
Highlight Criticality of Assets	8
Synchronize with your CMDB.....	9
Track Software, OS and hardware product lifecycle information	11
Manage authorized and unauthorized software	11
Define alerts for asset-related health issues	13
Generate Reports.....	14
Traffic Analyzer	15
I'm ready. How do I get started?	16
Download and install the Qualys Cloud Agent	16
Know the requirements	16
Which operating systems are supported?	16
Expand your Inventory	17
Scanners.....	17
Network Passive Sensor	18
CloudView	19
Secure Enterprise Mobility	20
Container Security	21
Shodan Assests.....	22

Introduction

CyberSecurity Asset Management (CSAM)/Global AssetView (GAV) continuously gather information on all assets, listing system and hardware details, running services, open ports, installed software and user accounts. Asset discovery and inventory collection is done through a combination of Qualys sensors, which together can collect comprehensive data from across on-premise or cloud infrastructure as well as remote endpoints

Qualys CyberSecurity Asset Management (formerly known as Global IT Asset Inventory) capabilities are available in two (2) versions:

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

GAV provides foundational inventory gathering capabilities for all assets in your hybrid IT environment, from on-premises servers and PCs, to Cloud instances, containers, Enterprise IoT and OT environments.

CSAM delivers additional capabilities on top of GAV to provide users with cybersecurity related content, such as product lifecycle information, ability to define authorized and unauthorized software and integration with ServiceNow CMDB among others. This helps you to accurately assess complex IT infrastructure and quickly identify and remediate risk.

Our free GAV service 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

Upgrade to CSAM and you'll also get: 

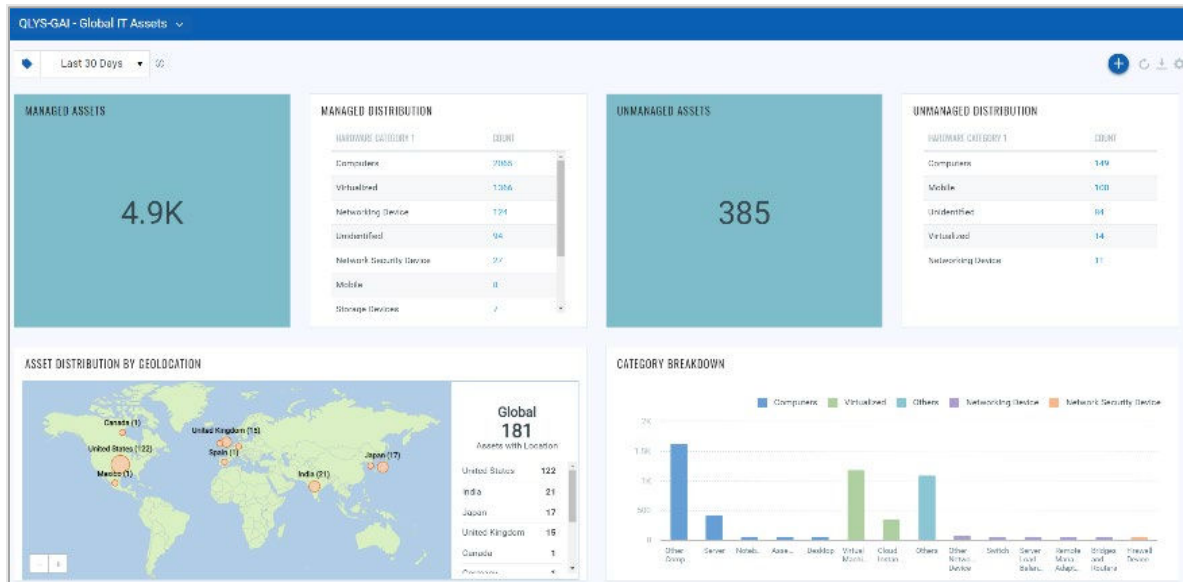
- Enriched asset data – hardware & software lifecycles, licenses categories, and more
- Bi-directional synchronization of asset data with your CMDB
- Ability to define and manage authorized and unauthorized software in your organization
- Customizable reporting to meet internal and external needs (e.g.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

Capabilities

The functionality available in GAV/CSAM can be divided into three (3) sets of capabilities:

Capabilities	Description
Discover and Inventory	<div> Discover and Inventory Use multiple Qualys sensors, including cloud agent to gain comprehensive asset inventory. Enrich it with business context from CMDB sync.</div> <p>Functionality to discover assets in your environment and collect inventory information about those assets.</p>
Detect and Monitor	<div> Detect and Monitor Detect software and hardware end of life, monitor unauthorized and missing required software.</div> <p>Functionality to detect potential asset health issues and monitor the health of your environment based on defined criteria.</p>
Report and Respond	<div> Report and Respond Define alerts, uninstall unauthorized software and produce compliance reports.</div> <p>Configuration of actions and reports related to your environment.</p>

Unlimited, continuous discovery GAV CSAM



Get ongoing updates on all assets, listing system and hardware details, active services, open ports, installed software and user accounts. Asset discovery and inventory collection is done through a combination of Qualys Network Scanners, Passive Sensors, Cloud Agents, and 3rd-party Connectors, which together can collect comprehensive data from across on-premises or cloud infrastructure and remote endpoints.

Normalization & categorization GAV CSAM



With GAV and CSAM, you can make your asset data consistent and uniform, which is essential for having inventory clarity and accuracy. The product standardizes manufacturer and product names, models and software versions by automatically normalizing raw discovery data using Qualys' ever-evolving technology catalog as reference. This process transforms the global IT asset inventory into multi-dimensional and structured information, so that you can make better business decisions. Inventory is also categorized by functional category and product families making it easy for you to review software and hardware based their function. For example, you can quickly identify all databases, or all routers in your environment, by filtering inventory data based on those categories.

Detailed asset information

GAV CSAM

The screenshot shows the 'Asset Details' page for an asset named 'win10-Last_locatio_test'. The page is divided into several sections:

- Asset Summary:** Displays the asset name, OS (Microsoft Windows 10 Pro 11009 Build 17763 64-bit), Hardware (VMware VMWare Virtual Platform), and Criticality Score (5).
- Identification:** Lists DNS Hostname (win10-Last_locatio_test), FQDN, NetBIOS Name (WIN10-auth-test1-updated), IPv4 Address (23.211.209.120), IPv6 Address, Asset ID (11104397), and Host ID.
- Activity:** Shows Last User Login (Administrator), Last System Boot (Sep 6, 2020 05:15 AM), Created On (Nov 18, 2021 03:02 PM), Last Updated (a day ago 07:41 AM), and Last Activity.
- Last Location:** A world map showing the asset's location. A tooltip indicates 'Location unknown. Last Seen: a day ago 07:41 AM'.
- Tags:** A list of tags including 'dynamicTag_3392_N...', 'dynamicTag_3392_U...', 'str', 'dynamicTag_3392_R...', 'Name-container-tag', 'dynamicTag_3392_L...', 'dynamicTag_3392_H...', 'dynamicTag_3392_J...', 'dynamicTag_3392_R...', 'dynamicTag_3392_T...', 'asset_test_locati...', 'test_123', 'dynamicTag_3392_G...', 'dynamicTag_3392_Z...', 'dynamicTag_3392_I...', 'dynamicTag_3392_D...', 'Name-container-tag', 'test_123', and 'dynamicTag_3392_R...'.

Automatically view detailed asset information, such as an assets' identity, running services, installed software, open ports, users, and more. GAV/CSAM gives you deep visibility into your assets granting you a detailed, multidimensional view of each one that encompasses both its IT and security data. You can flag issues such as configuration problems, security risks, IT policy violations and regulatory non-compliance with an asset profile that includes a wealth of data.

Powerful Search

GAV CSAM

The screenshot shows the 'Asset Inventory' search results page. The search query is 'software:(category1:'Databases' and lifecycle.stage:EOL)'. The results are displayed in a table with columns for 'Software Name', 'Category', 'Lifecycle Stage', 'Version', and 'Count'. The table shows several entries for 'Microsoft SQL Server Database Engine' with different versions and counts. The page also includes a sidebar with filters for 'Managed' (28 Total Software) and 'Lifecycle' (EOL, EOL/END, 19, EOL/END, 19).

Quickly find any asset, or information on an asset, in seconds for immediate answers. Our powerful search engine lets you craft simple or advanced queries combining multiple asset criteria returning results instantly.

GAV CSAM

As the inventory is building, you can start defining tags to easily find assets belonging to individual organization, performing roles or other groupings relevant to your organization. As you are creating tags, you can define criticality of your assets (e.g. Order Management System devices or executive team laptops should be defined as high criticality – 4 or 5)

Create New

Basic Details

Start with providing the following information to create your tag

Name *

Purchase Order System

☐

Mark as Favourite

Description

All devices used to deliver purchasing system

Asset Criticality Score

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

i

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

1

2

3

4

5

Tag Properties

Configure properties for your tag

Set Tag Color

Select Parent Tag

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

Create Tag

Tag Type

Static

Dynamic

For more information, refer [Configure Tags](#).

Highlight Criticality of Assets GAV CSAM

Apply tags manually or configure rules for automatic classification of your assets in logical, hierarchical, business-contextual groups. Assign Business Criticality through tags to establish priorities, and automatically calculates Asset Criticality Score (ACS) based on highest aggregated criticality.

Asset Details: win10-Last_locatio_test

Asset Summary

win10-Last_locatio_test
OS: Microsoft Windows 10 Pro (1809 Build 17763 64-Bit) | Criticality Score: 5
Hardware: VMware VMWare Virtual Platform

Identification

DNS Hostname: win10-Last_locatio_test
IP: 23.211.200.120
Last Seen: a day ago 07:41 AM

Activity

Last User Login: Administrator
Last System Boot: Sep 6, 2020 05:15 AM
Created On: Nov 18, 2021 03:02 PM

Location

Location unknown.
Last Seen: a day ago 07:41 AM

Asset Criticality Score

The highest score assigned to the asset via multiple tags is the asset criticality score of the asset.

Below are various scores assigned to the asset through multiple tags

Tag	Score
test	5
user.scope.tag1.w...	4

Tags

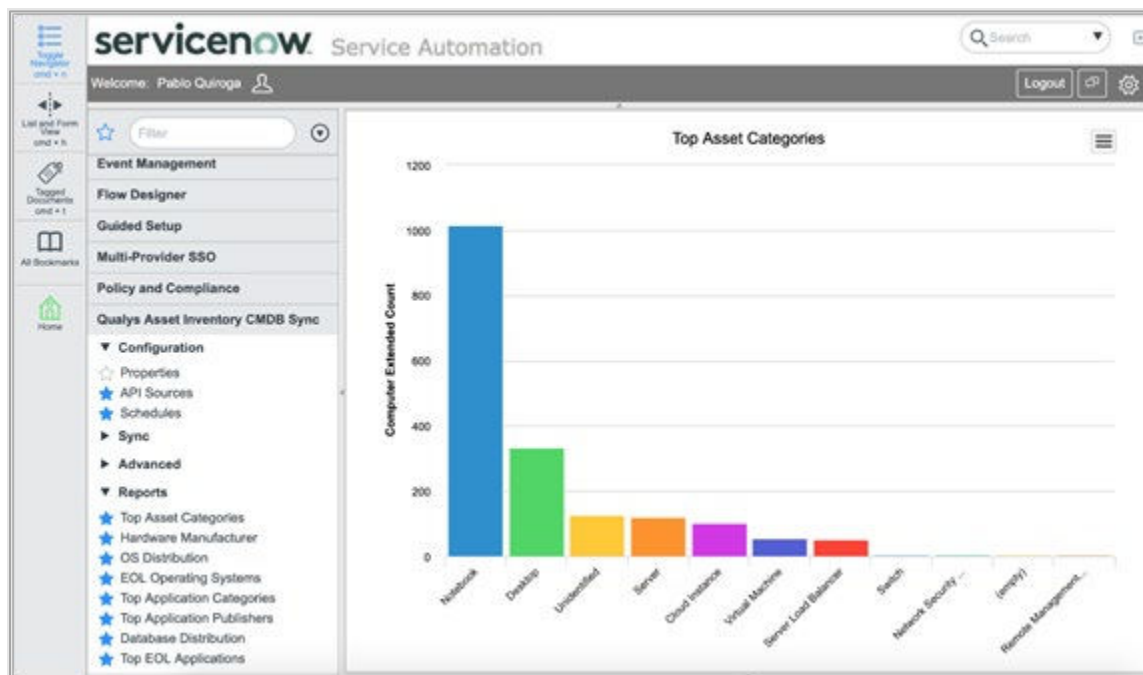
dynamicTag_3382_N... | dynamicTag_3382_U... | or | dynamicTag_3382_S... | Name contains tag |
dynamicTag_3382_2... | dynamicTag_3382_H... | dynamicTag_3382_J... | dynamicTag_3382_R... |
dynamicTag_3382_T... | asset_Last_locati... | Test_123 | dynamicTag_3382_O... | dynamicTag_3382_D... |
dynamicTag_3382_I... | dynamicTag_3382_O... | Name contains all | -1+1 | dynamicTag_3382_D...

Synchronize with your CMDB CSAM

You can ensure other users in your organization benefit from Qualys inventory by synchronizing inventory data with your CMDB. This will ensure that all users have access to the same, up-to-date information. CSAM inventory syncs with ServiceNow's CMDB, continuously feeding it fresh data, so the CMDB can accurately map assets' relationships, connections, hierarchies, and dependencies.

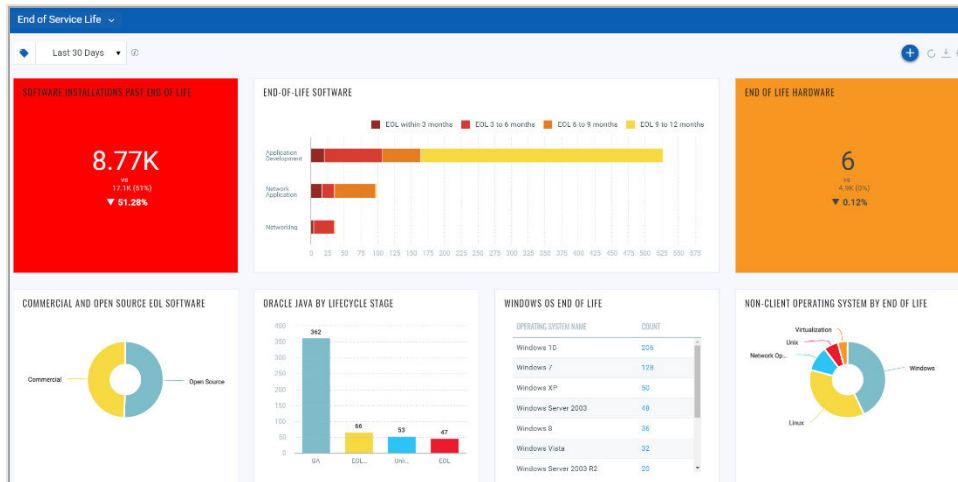
You can also enrich Qualys inventory with business information by importing business context to Qualys, including owners, environment, business applications and other key CMDB data to improve response to asset health issues. All using our ServiceNow-certified CMDB Sync App.

Get the [Qualys CMDB Sync Service Graph Connector App User Guide](#).



Track Software, OS and hardware product lifecycle information CSAM

Secure your environment by eliminating unsupported software and hardware. Review detailed hardware and software product lifecycle information to identify assets requiring replacement or upgrade. Gain additional context by identifying licensable and open source software.



Manage authorized and unauthorized software CSAM

Define and monitor authorized and unauthorized software installations in your environment. Define authorization rules for different parts of your environment (e.g. Firefox browser is authorized on personal computing devices, but unauthorized in the datacenter) to quickly identify potential security risks based on defined rules.

CyberSecurity Asset Management						
HOME DASHBOARD INVENTORY TAGS NETWORK RULES RESPONSES REPORTS						
Software Rules						
Recorder Create Rule Rules Software 1 - 50 of 540						
PRODUCT	PUBLISHER	CATEGORY	VERSIONS/UPDATES	AUTHORIZATION	RULE NAME	RULE STATUS
Brave	Brave Software	Network Application / Intern...	Below - Update 1.27.62	Authorized	testRule_JE630Z	Enabled
Microsoft Defender Advanced...	Microsoft	Security / Endpoint Protection	Specific - Update 10.5050.17763.771	Needs Review	testRule_JE630Z	Enabled
GOM Player	GOM & Company	Digital Content / Digital Vide...	Specific - Update 2.3.47.3309	Needs Review	testRule_JE630Z	Enabled
Zoom	Zoom Video Communications	Collaboration / Web Confere...	Between - Update 5.0.4 (25692.0524) 5.7.1 (543)	Unauthorized	testRule_JE630Z	Enabled
Chrome	Google	Network Application / Intern...	Specific - Update 79.0.3945.88	Unauthorized	testRule_JE630Z	Enabled
Plex Media Player	Plex	Digital Content / Computer ...	Above - Update 2.46.0.1031	Authorized	testRule_JE630Z	Enabled
Chrome	Google	Network Application / Intern...	Specific - Update 79.0.3945.88	Needs Review	CheckAny_Specific	Enabled
Zoom	Zoom Video Communications	Collaboration / Web Confere...	Specific - Version 5.7.4	Unauthorized	CheckAny_Specific	Enabled
Zoom	Zoom Video Communications	Collaboration / Web Confere...	Above - Update 5.6.7 (1016)	Authorized	Mapper_check	Enabled
GOM Player	GOM & Company	Digital Content / Digital Vide...	ANY - Update	Needs Review	Mapper_check	Enabled
GOM Player	GOM & Company	Digital Content / Digital Vide...	Specific - Version 2.1	Needs Review	Mapper_check	Enabled
Chrome	Google	Network Application / Intern...	Above - Version 81.0	Unauthorized	Mapper_check	Enabled

As you continue to review your inventory, you can start defining Software Authorization Rules (Rules tab). You can create new authorization rules in two (2) ways:

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

As you are creating the rules, you can define the scope of the authorization (e.g. Firefox browser is authorized on personal computing devices, but unauthorized on server devices). You can create as many rules as you need. Once rules are created, they are evaluated in priority order as you may have conflicting rules based on device selection (e.g. you could unauthorized Firefox on all devices, then authorize Firefox for use by the engineering team on their devices). In this example, you will need to place global unauthorized rule below authorization rule for the engineering team.

Add Software to Authorization Rule

Track the software product as authorized/unauthorized

Chrome
Network Application / Internet Browser

☒ This Update (79.0.3945.88) ☐ Entire Product

Authorization *

Select the value ▼

	ORDER NUMBER	RULE	STATUS	TAGS
<input type="radio"/>	1	testRule_JE63OZ	Disabled	auto_authUnauth.8.
<input type="radio"/>	2	CheckAny_Specific	Enabled	sk3
<input type="radio"/>	3	Mapper_check	Enabled	sk3

Cancel

Create New Rule

Save

For more information, refer [Track Authorized/Unauthorized Software](#).

Define alerts for asset-related health issues CSAM

Configure email, Slack or PagerDuty alerts to notify users about asset health issues requiring their attention including product lifecycle, software authorization or other items such as open ports or insufficient server storage.

The screenshot shows the 'Rule Details' form in Qualys Global AssetView. A modal window titled 'Sample Queries' is open, displaying three sample queries to help get started. The background form is partially visible, showing fields for 'Rule Name', 'Description', 'Rule Query', and 'Action Settings'.

Rule Details
Provide the following information to create the rule

Note: Alert e...

Rule Information

Rule Name *
Database EOS for 1

Description *
Database EOS

Rule Query
Provide a query to m...

Rule Query *
software: (ca...

Sample Queries

Some Sample Queries to help you to get started

- ☐ **Unauthorized Software**
Found unauthorized software
software:(authorization:'Unauthorized' and firstFound:[now-1d ... now])
- ☐ **Database EOS**
Database is reaching End-of-Service (EOS) on 180th day from today
software:(category1:'Databases' and component:'Server' and lifecycle.eos:[now+179d ... now+180d])
- ☐ **Operating System EOS**
Server's Operating System is 180th day away of reaching End-of-Service (EOS) from today
operatingSystem.category2:'Server' and operatingSystem.lifecycle.eos:[now+179d ... now+180d]

☐ Internet facing assets ports

Action Settings
Choose an appropriate...

Actions *
Email for Database EOS

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.).

Qualys supports three (3) mechanisms for alerting:

- Email
- Slack
- PagerDuty

For more information, refer [Configure Responses](#).

Generate Reports CSAM

Create and share inventory reports with internal stakeholder using provided and custom templates. Mandates like FedRAMP and PCI require you to track all assets and software, as well as continuously monitor their security gaps. Easily generate reports so you can demonstrate compliance. Reporting includes configurable out-of-the-box templates, for example to address FedRAMP requirements.

← Create New : FedRAMP Template

STEPS 5/5

1 Basic Details

2 Report Source

3 Report Display

4 Report Schedule

5 Summary

Review and Confirm

Review and Confirm your selections

⌵ Basic Details

Specify report title and description

Name

Compliance Report

Description

Description of the report

⌵ Report Source

Specify assets or assets tags to include in your report

Search Query

-

⌵ Report Display

Select the columns you want to show in your report

Selected Columns

Software Information

All

Host Information

All

⌵ Report Schedule

Set the run and delivery of this report

Schedule Type

On Demand

Timezone

(GMT 05:30) India Standard Time (IST Asia/Kolkata)

Cancel

Previous

Confirm

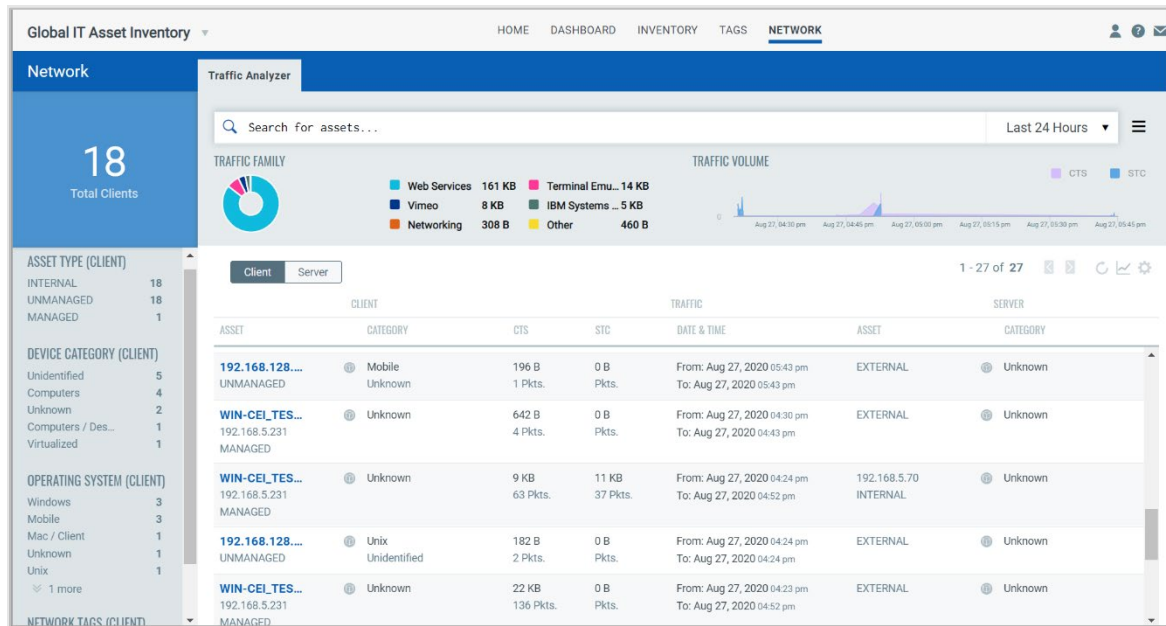
You can also generate reports to provide information about your environment to internal or external stakeholders using our reporting function.

For more information, refer [Generate Reports](#).

Qualys Global AssetView | Qualys CyberSecurity Asset Management

14

Traffic Analyzer



Traffic Analyzer requires Network Passive Sensor and provides a detailed and consolidated view for the traffic in your network. This helps you to understand the communication between different assets in your environment. For example, communication of certain type of an unmanaged asset from unsecured network to a critical resource. It also shows date wise traffic volume summary for client to server (CTS) and server to client (STC) in tabular and graphical view. It provides graphical views of the traffic categorized by family and by volume. It shows all traffic flow details for both managed and unmanaged assets.

For each flow, one can pivot to any of the two assets participating in the traffic flow to check the details such as asset summary, network information, system information, list of open ports and traffic summary of an asset.

For more information, refer [Traffic Analyzer](#).

I'm ready. How do I get started?

Download and install the Qualys Cloud Agent

Start building your inventory by installing cloud agents. With our lightweight agents you'll get continuous network security updates through the cloud. As soon as changes are discovered on your hosts they'll be assessed and you'll know about new security threats right away.

You can have cloud agents on private clouds, public clouds, on premise and endpoints to continuously discover your IT assets providing 100% real-time visibility.



Know the requirements

Here are the requirements for installing and running Cloud Agent on your system:

- Host must reach Qualys Cloud Platform (or Qualys Private Cloud Platform) over HTTPS port 443
- (Windows) Local administrator privileges on the host. Proxy configuration is supported.
- (Linux, Mac, AIX) Root privileges, non-root with sudo root delegation, or non-root with sufficient privileges. Proxy configuration is supported.

Which operating systems are supported?

You can install cloud agents on Windows, Linux, MacOS, PowerPC and AIX.

On the [Qualys Documentation portal](#), under **Sensors > Cloud Agents**, refer to the [Cloud Agent Getting Started Guide](#) and installation guides for different platforms.

Expand your Inventory

Use other Qualys solutions to expand your inventory:

- Scanners to discover and inventory systems remotely using credential-based scans.
- Network Passive Sensor to discover unknown devices in the network.
- CloudView to expand with cloud resource information,
- Secure Enterprise Mobility to expand with mobile devices, and
- Container Security to gain insights into containerized applications in your environment.
- Synchronize with Shodan to get attack surface visibility

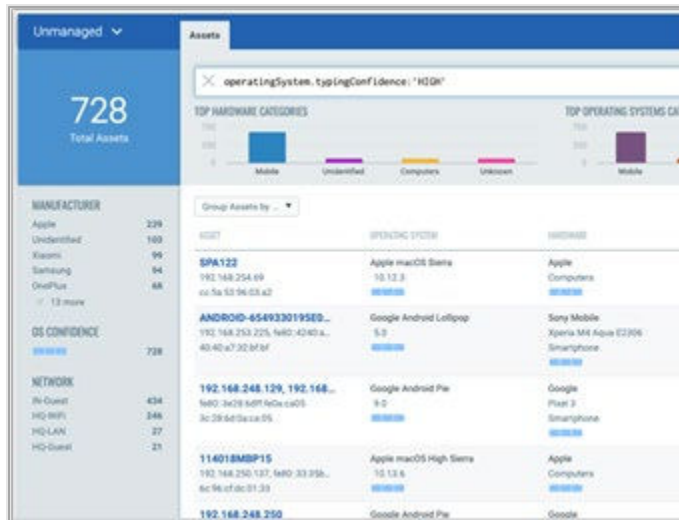
Scanners

With the Qualys Scanner Appliance, you can assess internal network devices, systems and web applications. The Scanner Appliance is a robust, scalable solution for scanning networks of all sizes including large distributed networks. Refer to the [Scanner Appliance User Guide](#) for installation and configuration information.

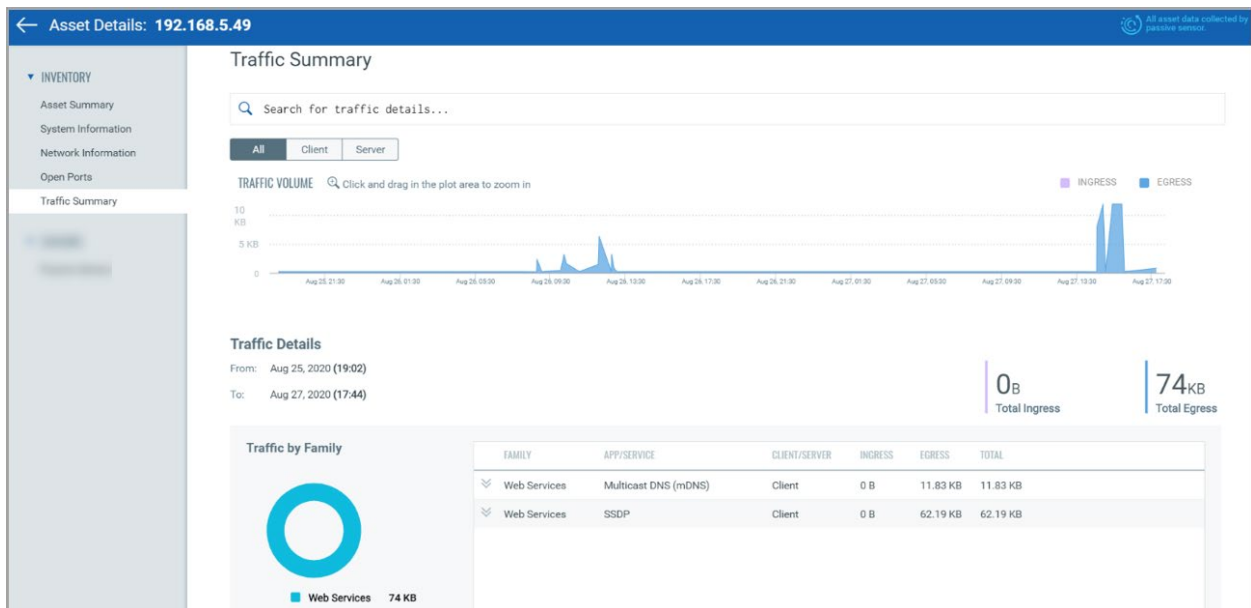
Scans									
Scans Maps Schedules Appliances Option Profiles Authentication Search Lists Setup									
New	Search	1 - 20 of 21							
Network	Appliance	Personalization Code	LAN IP	WAN IP	LAN IPv6	polling	Scanner	Signatures	Last Update
MCW-Test 2	AI/VS-Demo-AS1-Scanner	20524394632606	172.31.0.58	--	--	180 seconds	12.4.34-1	2.5.234-3	07/15/2021 at 09:40:11 AM (GMT-0400)
Europa-US	AI/VS-Demo-UE1-Scanner	20560608502284	10.0.0.15	--	--	180 seconds	12.4.34-1	2.5.234-3	07/15/2021 at 11:18:07 AM (GMT-0400)
Global Default Network	AI/VS-Golden-AM-Pipeline-uswest1	20526013007213	10.100.1.28	--	--	180 seconds	11.9.24-1	2.4.911-4	09/16/2020 at 01:40:31 PM (GMT-0400)
Global Default Network	AZURE-Demo-EastUS2-Scanner	20556547486326	10.2.0.7	--	--	180 seconds	12.4.34-1	2.5.234-3	07/15/2021 at 10:51:10 AM (GMT-0400)
Global Default Network	AZURE-Demo-WESTUK-Scanner	20576365780651	10.0.1.12	--	--	180 seconds	12.4.34-1	2.5.234-3	07/15/2021 at 07:33:12 AM (GMT-0400)
Global Default Network	AZURE_US1	20565877853325	--	--	--	180 seconds	--	--	N/A
BU-Atlanta-Network: 192.168.1/24	BU-Atlanta-VS	20596123500117	192.168.1.29	--	--	180 seconds	12.1.67-1	2.4.907-2	09/21/2020 at 06:37:06 AM (GMT-0400)
BU-DC-ONPREM-AZ	BU-DC-ONPREM-AZ-Scanner	20576779065074	10.0.1.132	--	fd00:9e91:dc07:1:20c:2fff:fe3:49ed64	180 seconds	11.7.45-1	2.4.777-2	12/25/2019 at 07:55:06 PM (GMT-0500)
BU-NET-ACS-LABs	BU-NET-ACS-LABs-ScannerV1	20577193682891	10.113.210.215	--	--	180 seconds	12.4.34-1	2.5.234-3	07/15/2021 at 09:25:12 AM (GMT-0400)
Global Default Network	GCP-Demo-AG1-Scanner	20579042716601	192.168.0.130	--	--	180 seconds	12.4.34-1	2.5.234-3	07/15/2021 at 06:43:09 AM (GMT-0400)
Global Default Network	GCP-Demo-UV2-Scanner	20575790218613	10.0.0.138	--	--	180 seconds	12.4.34-1	2.5.234-3	07/15/2021 at 07:41:08 AM (GMT-0400)
Global Default Network	POX_InternalEd	20504353273627	10.0.0.89	--	2601:1e0:6901:2e40:a00:27ff:fe0c:e9cd64	180 seconds	12.3.51-1	2.5.159-3	04/16/2021 at 03:11:57 PM (GMT-0400)
Global Default Network	QVSA Training Qualys.com	20529105754525	10.116.133.44	--	--	180 seconds	12.4.34-1	2.5.234-3	07/15/2021 at 11:05:08 AM (GMT-0400)
Global Default Network	RDLAB_USA_Scanner-PC-1	20551003496039	10.10.22.121	--	--	180 seconds	12.4.34-1	2.5.234-3	07/15/2021 at 10:01:08 AM (GMT-0400)
BU-NET-RDLABs	RDLAB_USA_Scanner1	20506177528006	10.10.22.122	--	--	180 seconds	12.4.34-1	2.5.223-4	07/02/2021 at 11:18:49 AM (GMT-0400)
BU-NET-RDLABs	RDLAB_USA_Scanner3	20528004708389	10.11.49.204	--	--	180 seconds	12.4.34-1	2.5.223-3	07/15/2021 at 09:50:28 AM (GMT-0400)
BU-NET-RDLABs	RDLAB_INDIA_Scanner1	20541585182878	10.115.51.181	--	--	180 seconds	12.4.34-1	2.5.234-3	07/15/2021 at 07:54:13 AM (GMT-0400)
BU-NET-RDLABs	RDLAB_INDIA_Scanner2	20540483073351	10.115.49.134	--	--	180 seconds	12.4.34-1	2.5.234-3	07/15/2021 at 09:53:12 AM (GMT-0400)
Global Default Network	rr	20590001064397	--	--	--	180 seconds	--	--	N/A
Global Default Network	test15	20554698040807	--	--	--	180 seconds	--	--	N/A

Network Passive Sensor

Identify known and unknown devices the moment they connect to your network, eliminating blind spots across your IT environment. Refer to [Network Passive Sensor Getting Started Guide](#) for additional information.



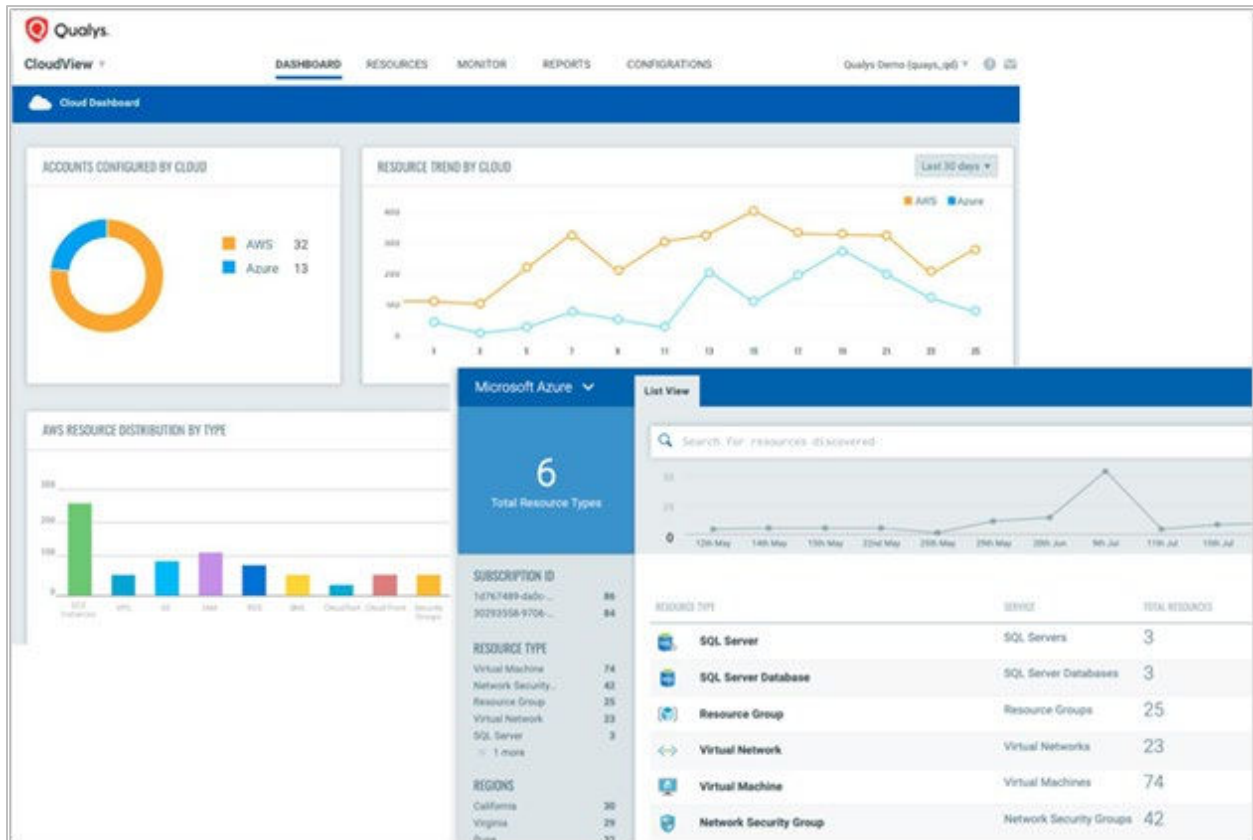
- Identify and profile assets the moment they connect to your network
- Understand network traffic across your environments to help detect unusual activity



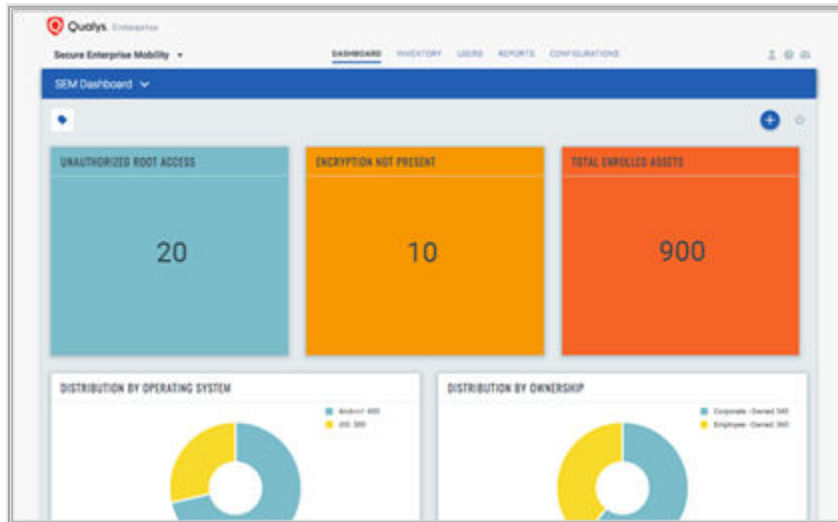
CloudView

Qualys CloudView provides continuous inventory of your public cloud workloads and infrastructure. For more information, refer [CloudView User Guide](#).

- Get comprehensive visibility of your public cloud resources
- Works across Amazon Web Services, Google Cloud and Microsoft Azure
- Easily upgrade to get continuous compliance assessments

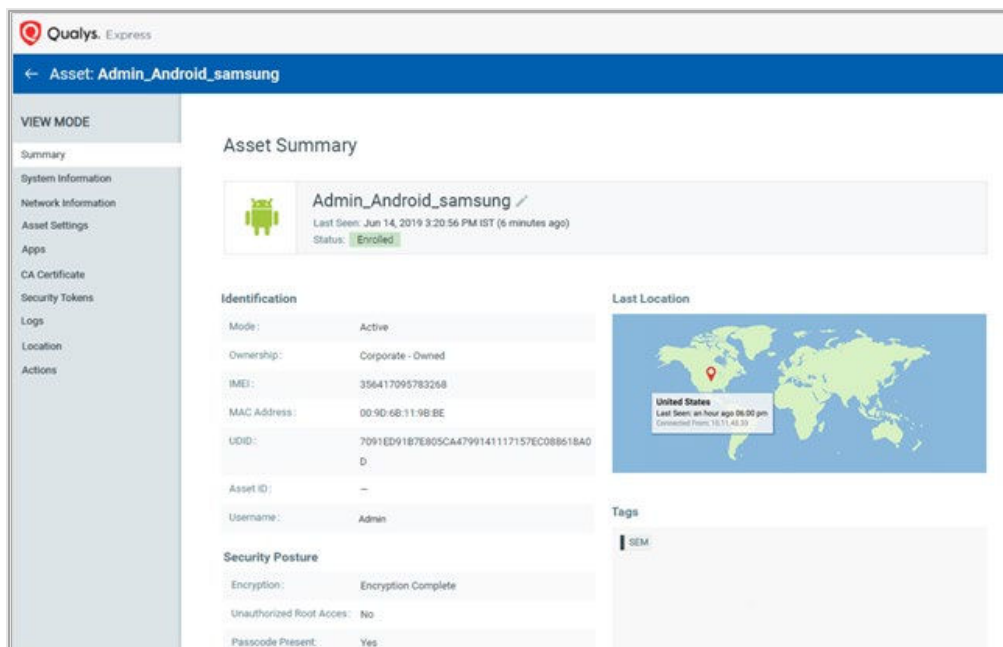


Secure Enterprise Mobility



Qualys SEM provides complete visibility, security and continuous monitoring for your mobile devices and data.

- Complete visibility for corporate-owned devices and BYOD
- Works with Android and iOS
- Easily upgrade to get vulnerability management and mobile data security



Container Security

Qualys Container Security provides discovery, tracking, and continuously protecting container environments. Upon installation of the sensor, it automatically scans the host for the images and containers that are present on the host. The inventory and the metadata of the inventory is pushed to your Qualys Cloud Platform account. We'll help you get started quickly!

The Assets section lists the Images and Containers discovered along with their metadata information like ports, networks, services, users, installed software, etc. The assets are listed along with their associations like associated containers and hosts for an image, other containers from the same parent image. Users can search for images and containers based on their attributes.

← Asset Details: centos

▼ INVENTORY

Asset Summary

System Information

Network Information

Open Ports

Installed Software

Business Information


▼ SECURITY

Vulnerabilities

Certificates

Container Security

Container Summary



Docker version:

18.09.0-beta5

Assoc. containers:

1

Assoc. images:

28

Shodan Assests CSAM

Integration with third-party sources like Shodan.io gives an outside-in view to find assets exposed to the internet, flagging known 'managed' assets, identifying unknown assets, and enabling security risk assessment.

With this capability, you can:

- Pull customer-specific public data from Shodan
- Display it in the Asset Inventory and Asset Details
- Create Unmanaged Assets to track newly identified endpoints
- Enable contextual queries

Here, you can import assets from Shodan to your inventory. We have added an option on the Home page to activate Shodan and manage Shodan configurations to import assets based on the filters in the configuration.

The screenshot shows the CyberSecurity Asset Management (CSAM) interface. The top navigation bar includes 'Dashboard', 'Inventory', 'Tags', 'Rules', 'Responses', and 'Reports'. The 'Inventory' section is active, showing a search bar and a filter for 'Last 30 Days'. The main content area displays a table of assets. The table has columns for 'Asset', 'Criticality', 'Operating System', 'Hardware', 'Last User', 'Sources', 'Modules', and 'Tags'. A red box highlights the 'Sources' column for the asset 'win10-Last_location_test', showing a 'SHODAN' source with 'First Found: Nov 11, 2021' and 'Last Seen: Nov 23, 2021'. The left sidebar shows '34 Total Assets' and various filters like Manufacturer, Tags, and Sources.

ASSET	CRITICALITY	OPERATING SYSTEM	HARDWARE	LAST USER	SOURCES	MODULES	TAGS
Auto-centos-ip-after-fix 10.115.71.152,172.17.0.1 02:42:e9:a4:86:5e	2	The CentOS Project CentOS 7 1611	VMware VMware Virtual Platform Virtual Machine	root	First Found: Oct 14, 2020 Last Seen: Dec 21, 2021	CSAM VM	Business_ID 5 more...
test50034 172.20.0.5 00:00:34:43:56:43	5	Microsoft Windows Server 2016 1607	Microsoft Azure GSV-series Standard_DS... Cloud Instance		SHODAN First Found: Nov 11, 2021 Last Seen: Nov 23, 2021	CSAM VM	DynamicTag_3382_J... 26 more...
win10-Last_location_test 23.211.200.120 00:50:56:AA:80:02	5	Microsoft Windows 10 Pro1809 Build 17763 64-bit	VMware VMware Virtual Platform Virtual Machine	Administrator	First Found: Nov 11, 2020 Last Seen: Jan 09, 2022	CSAM VM	DynamicTag_3382_J... 27 more...
BSApps-Webserver 10.40.2.119 0a:c1:a0:a4:3a:c1	4	Microsoft Windows	Amazon Web Services Amazon EC2 T2 12 micro Cloud Instance		First Found: Mar 26, 2021 Last Seen: Jan 10, 2022	CSAM	BusinessApp-Name-Tag 27 more...
BSApps-Windows-EC2 10.40.2.88 0a:c1:a0:a4:3a:c1	5	Microsoft Windows	Amazon Web Services Amazon EC2 T2 12 micro Cloud Instance		First Found: Mar 27, 2021 Last Seen: Jan 10, 2022	CSAM	id 10 more...