Qualys Global AssetView
CyberSecurity Asset Management
Quick Start Guide

August 5, 2022
Table of Contents

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 Assets .................................................................................... 22
  External Attack Surface Management (EASM) Assets ...................... 22
Introduction

CyberSecurity Asset Management (CSAM)/Global AssetView (GAV) continuously gathers information on all assets, listing system and hardware details, running services, open ports, installed software, and user accounts. Asset discovery and inventory collection are 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, the 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:

<table>
<thead>
<tr>
<th>Capabilities</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discover and Inventory</td>
<td>Functionality to discover assets in your environment and collect inventory information about those assets.</td>
</tr>
<tr>
<td>Detect and Monitor</td>
<td>Functionality to detect potential asset health issues and monitor the health of your environment based on defined criteria.</td>
</tr>
<tr>
<td>Report and Respond</td>
<td>Configuration of actions and reports related to your environment.</td>
</tr>
</tbody>
</table>
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 are 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

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 a 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 on their function. For example, you can quickly identify all databases, or all routers in your environment, by filtering inventory data based on those categories.
Automatically view detailed asset information, such as an asset’s 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.

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.
Create asset tags and define asset criticality

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

For more information, refer to Configure Tags.
Highlight Criticality of Assets

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 the highest aggregated criticality.
Synchronize with your CMDB

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.
<table>
<thead>
<tr>
<th>Name</th>
<th>NetBIOS name</th>
<th>IP Address</th>
<th>Os Category</th>
<th>Os Name</th>
<th>Os Lifecycle Stage</th>
<th>Hardware category</th>
<th>Hardware Full Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>dk000450</td>
<td>DKTP00450</td>
<td></td>
<td>Windows / Server</td>
<td>Windows 2016</td>
<td>GA</td>
<td>Computers / Notebook</td>
<td>Lenovo ThinkPad T4 20FKA03000</td>
</tr>
<tr>
<td>dk000428</td>
<td>DKTP00428</td>
<td>10.145.87.80</td>
<td>Windows / Server</td>
<td>Windows 2008 Service Pack 2</td>
<td>EOL</td>
<td>Computers / Notebook</td>
<td>Lenovo ThinkPad T4 20FWS0070US</td>
</tr>
<tr>
<td>dk000415</td>
<td>DKTP00415</td>
<td></td>
<td>Windows / Embedded</td>
<td>Windows 7 Embedded Service Pack 1</td>
<td>EOL</td>
<td>Computers / Notebook</td>
<td>Lenovo ThinkPad T4 20FWS0070US</td>
</tr>
<tr>
<td>dk000399</td>
<td>DKTP00399</td>
<td>12.48.105.83</td>
<td>Windows / Client</td>
<td>Microsoft(R) Windows(R) XP Professional ...</td>
<td>EOL/EOS</td>
<td>Computers / Notebook</td>
<td>Lenovo ThinkPad T4 20BEX0071US</td>
</tr>
<tr>
<td>dk000402</td>
<td>DKTP00402</td>
<td>12.64.174.186</td>
<td>Windows / Server</td>
<td>Windows 2016/10</td>
<td>GA</td>
<td>Computers / Notebook</td>
<td>Lenovo ThinkPad T4 20BX0011US</td>
</tr>
<tr>
<td>dk000382</td>
<td>DKTP00382</td>
<td>11.91.88.219</td>
<td>Windows / Server</td>
<td>Windows 2012 R2 Standard</td>
<td>EOL</td>
<td>Computers / Notebook</td>
<td>Lenovo ThinkPad T4 20BV0000US</td>
</tr>
</tbody>
</table>
**Track Software, OS, and hardware product lifecycle information**

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.

![Software Lifecycle Tracking]

**Manage authorized and unauthorized software**

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 data center) to quickly identify potential security risks based on defined rules.

![Software Rules Management]

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 the Rules tab and creating a 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 the global unauthorization rule below the authorization rule for the engineering team.

For more information, refer to Track Authorized/Unauthorized Software.
Define alerts for asset-related health issues

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.

To effectively manage your inventory, you should set up 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 to Configure Responses.
Generate Reports

Create and share inventory reports with internal stakeholders 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.

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

For more information, refer to Generate Reports.
Traffic Analyzer requires Network Passive Sensor and provides a detailed and consolidated view of 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 unmanaged asset from an unsecured network to a critical resource. It also shows a date-wise traffic volume summary for the client to server (CTS) and server to client (STC) in a 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 to 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.
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 a continuous inventory of your public cloud workloads and infrastructure. For more information, refer to 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 are 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, and other containers from the same parent image. Users can search for images and containers based on their attributes.
Shodan Assets

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.

External Attack Surface Management (EASM) Assets

Qualys CyberSecurity Asset Management (CSAM) provides comprehensive visibility in the form of External Attack Surface Management (EASM). It gives an outside-in view of your external-facing IT infrastructure to continuously monitor your organization’s external attack surface and internet-connected assets, track changes, and receive notifications when new assets, unknown assets, or critical issues are found. Also, it allows you to continuously identify and assess the security and compliance gaps of your organization’s network.

Note: EASM is a new Beta feature. It’s in early preview and available on a request basis.

External Attack Surface Management (EASM) gives you comprehensive visibility to monitor the external-facing organization’s infrastructure network to discover the vulnerable systems, target attacks, and campaigns.

With this capability, you can:

- Discover all your domains, subdomains, subsidiaries, and the assets associated with it
- Discover unsolicited ports, certificates, and applications running on exposed assets
- Identify potential vulnerabilities and weaknesses on exposed assets

As shown in the following screen capture, you can view the inventory of the EASM discovered assets.

Go to the CSAM online help to know more detailed information about how to add and manage EASM configuration to discover sets from EASM.