Qualys CyberSecurity Asset Management

Playbook

August 9, 2022

Qualys, Inc.
919 E Hillsdale
Blvd4th Floor
Foster City, CA
944041 (650) 801
6100

Table of Contents

Qualys CyberSecurity Asset Management Playbook

Qualys CyberSecurity Asset Management 2.0 (CSAM) launched External Attack Surface Management; asset management reimagined for security teams. With Qualys CSAM, organizations gain a complete view of their internal and internet facing exposures, can continuously inventory assets, apply business criticality, and risk context, detect security gaps like unauthorized or EOL software, and respond with appropriate actions to mitigate risk, thus reducing the 'threat debt'.

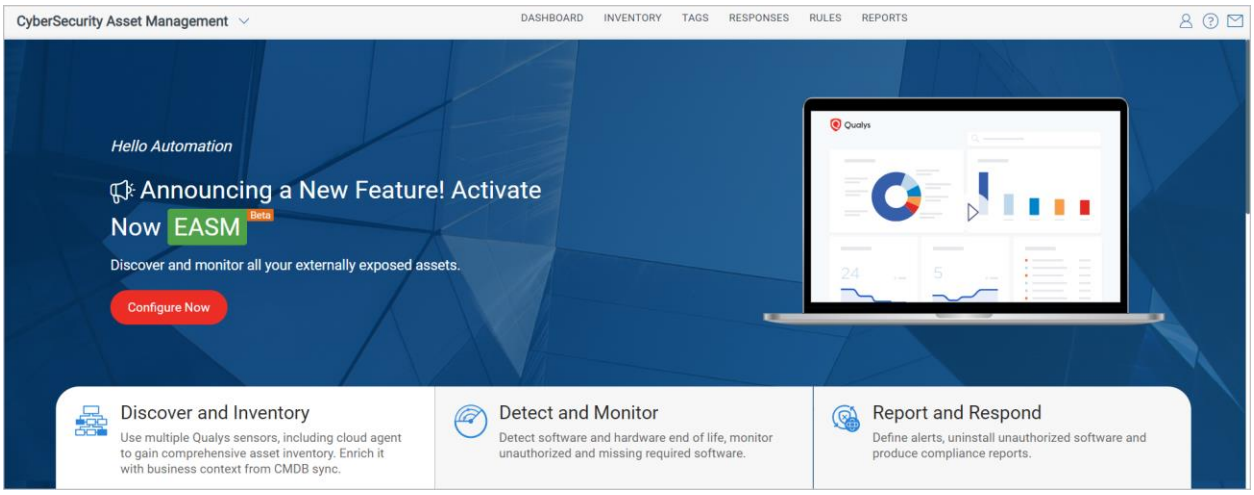
Cyber Security Asset Management 2.0 with External Attack Surface Management enables organizations to continuously monitor and reduce the entire enterprise attack surface including internal and internet facing assets, discover previously unknown exposures, synchronize with CMDBs, detect security gaps like unauthorized or end-of-support software, and respond with appropriate actions to mitigate risk.

Introducing CyberSecurity Asset Management
Reinventing Cybersecurity Asset Management

Refer Qualys blogs to know more about CSAM and to Qualys Documentation to set up and configure Qualys apps, as required.

Let's Get Started

CSAM provides cybersecurity-related material such as product lifecycle information, the ability to define allowed and unauthorized software, and integration with ServiceNow CMDB, among other things. With CSAM, you'll identify all systems comprehensively, detect at-risk assets, and respond with appropriate actions to mitigate risk.

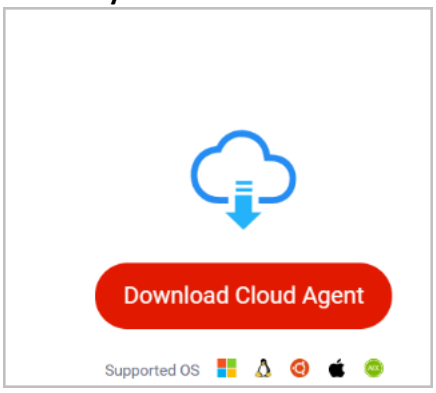


Discover and Inventory - Discover assets in your environment and collect inventory information about those assets.
Detect and Monitor - Detect potential asset health issues and monitor the health of your environment based on defined criteria.
Report and Respond - Configure actions and reports related to your environment.

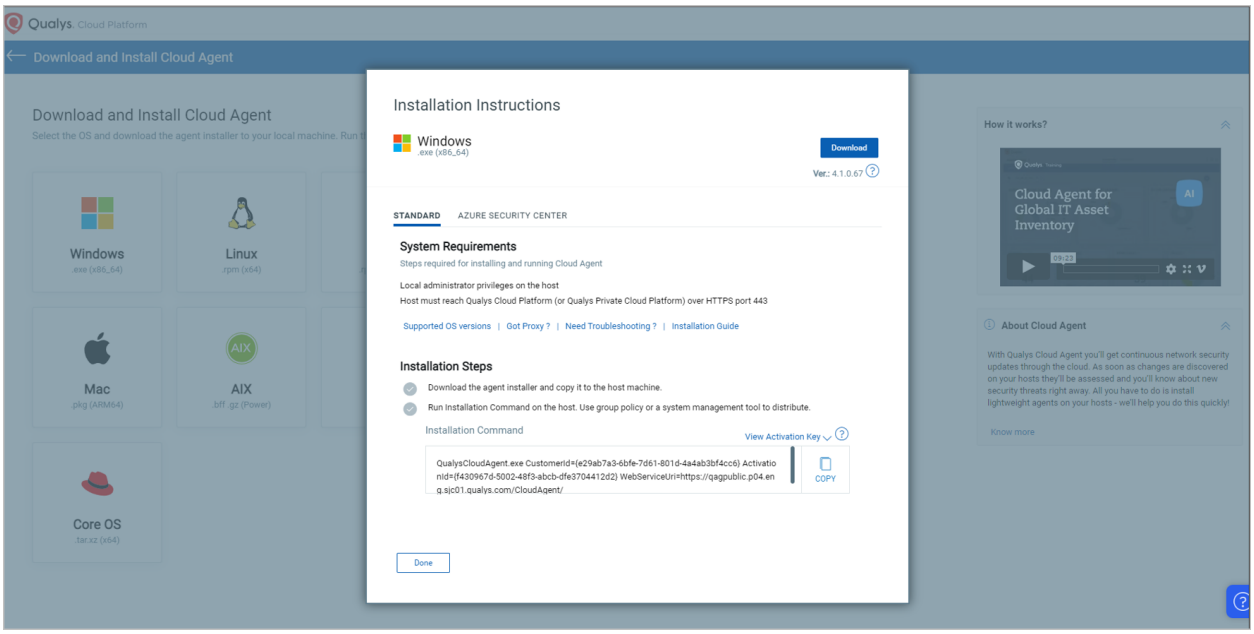
Step 1 - Get started by installing cloud agents

Start building your inventory by installing cloud agents. You can install cloud agents on Windows, Linux, MacOS, Unix, PowerPC, and AIX platforms.

Navigate to the **Home** page and click the **Download Cloud Agent** button from the **Discovery and Inventory** tab.



Click Windows and follow the agent installation instructions displayed on the page. We provide you with a default AI activation key for the agent installation. To add or manage your keys, go to **Cloud Agent** > **Agent Management**.



Step 2 - Expand your inventory with other Qualys sensors

After completing the installation of cloud agents, now is the time to scale up your inventory. You can use additional Qualys solutions to expand your inventory like: –

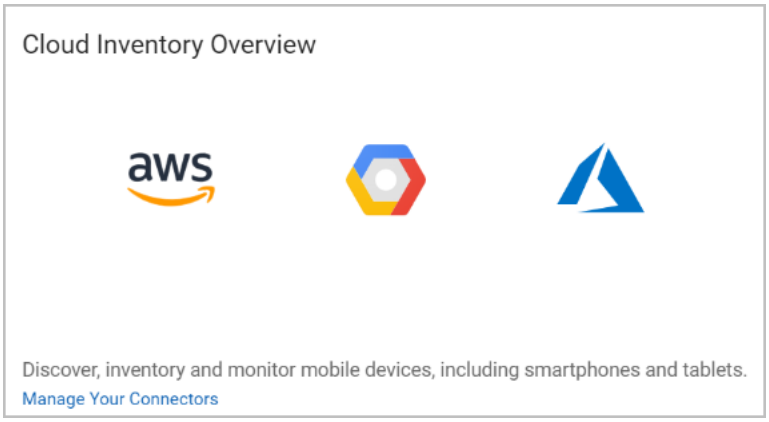
1. CloudView to expand with cloud resource information,
2. Secure Enterprise Mobility to expand with mobile devices,
3. Network Passive Sensor to discover unknown devices in the network.

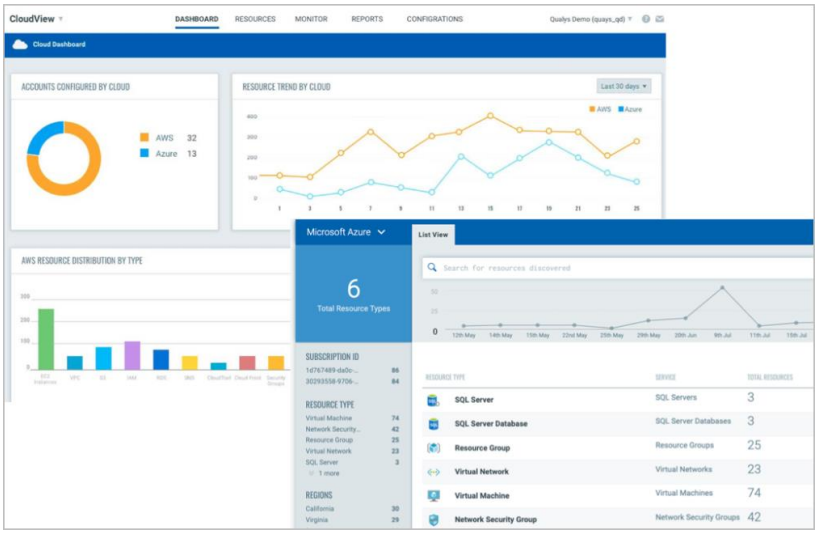
Qualys CloudView

Qualys CloudView provides continuous inventory of your public cloud workloads and infrastructure.

Start Here

Click **Manage Your Connectors** from the **Cloud Inventory Overview** section of the **Discover and Inventory** tab.





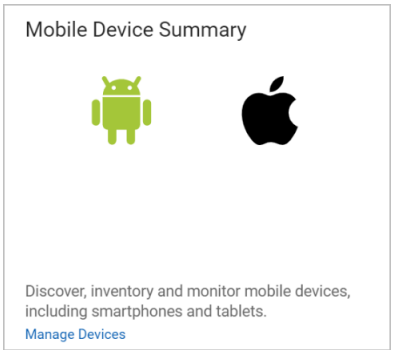
If you already have CloudView, you can create connectors in CloudView and view your CloudView assets in your Inventory tab.

Refer to the Qualys CloudView User Guide and associated documentation to setup your account and create connectors in CloudView.

Security Enterprise Mobility (SEM)

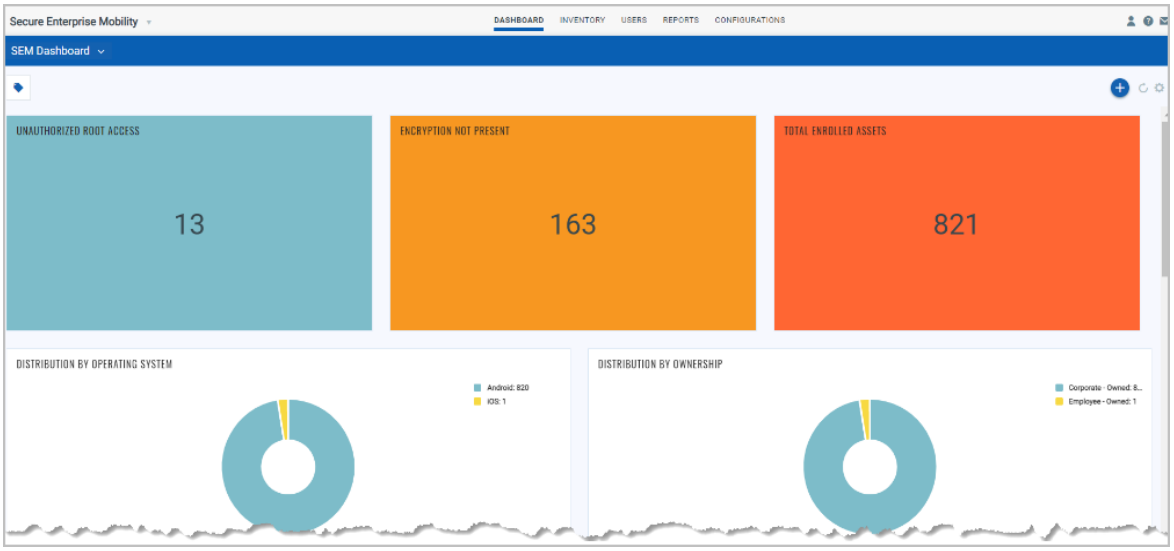
Qualys Secure Enterprise Mobility (SEM) offers you a cloud-based solution, to help you secure, monitor, and manage mobile devices.

From the CSAM, click **Manage Devices** in the **Mobile Devices Summary** section under the **Discover and Inventory** tab.



Then from the SEM app you will need to do the following to set up your mobile assets:

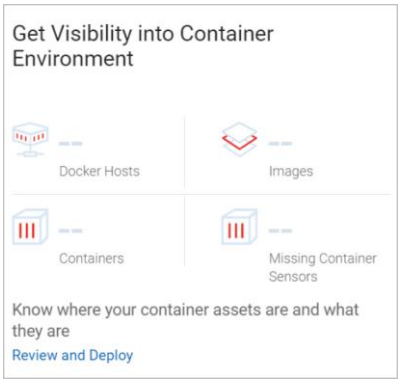
1. Set up the EULA from the Configuration tab.
2. Create user accounts in the Users tab.
3. Install the Qualys QAgent app on devices and enroll the devices into the application.
4. You can now start monitoring your devices on the Dashboard.



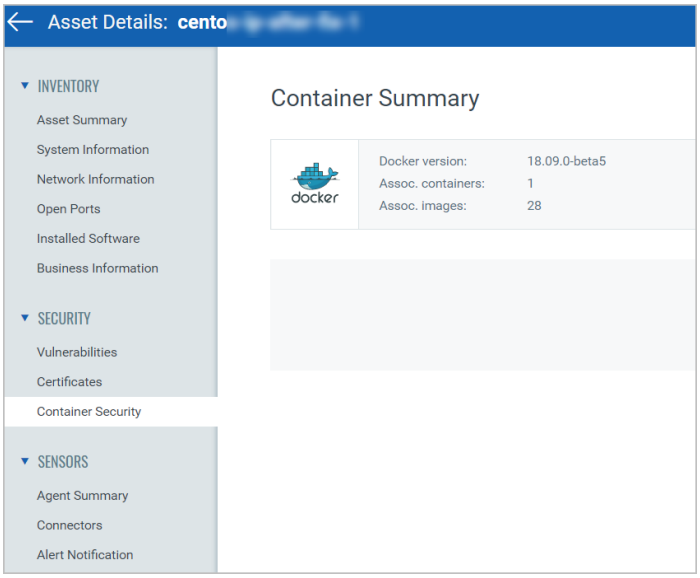
Container Security

Qualys Container Security provides discovery, tracking, and continuously protecting container environments.

From the CSAM, click **Review and Deploy** in the **Get Visibility into the Container Environment** section under the **Discover and Inventory** tab.



The Assets section lists the Images and Containers discovered along with their metadata information like ports, networks, services, users, installed software, etc.

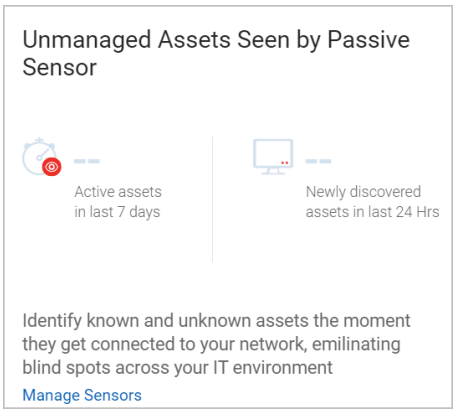


For more information, refer Container Security User Guide.

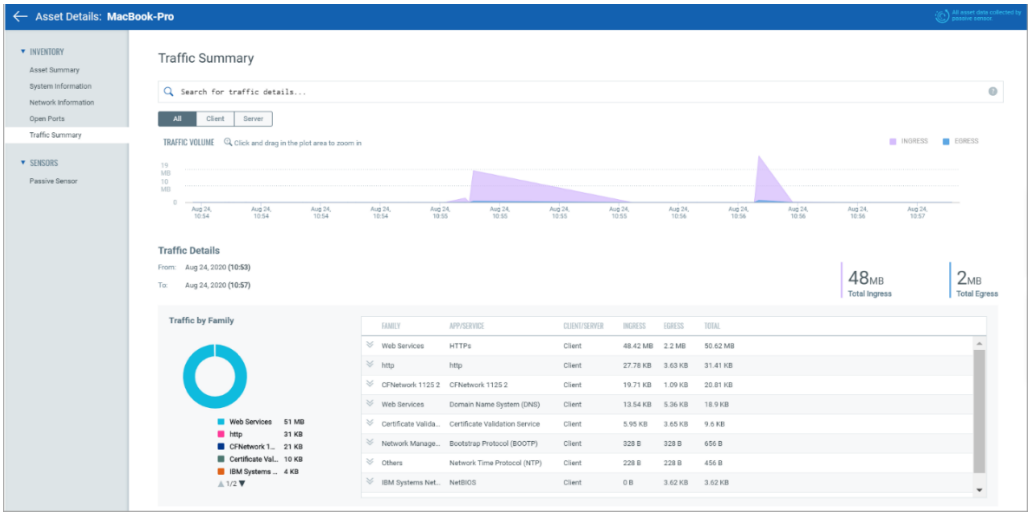
Network Passive Sensor

Network Passive Sensor (PS) helps you to automatically detect and profile all network-connected systems, eliminating blind spots across your IT environment.

From the CSAM, click **Manage Sensors** in the **Unmanaged Assets Seen by Passive Sensor** section under the **Discover and Inventory** tab.



Understand and identify known and unknown assets the moment they connect to your network.



Step 3 – Integrate with ServiceNow CMDB to receive full asset data

Now that you've set up inventory, by synchronizing data with your CMDB you can add security and business context to asset inventory. You can schedule synchronization of asset metadata from ServiceNow to Qualys. You can update your CMDB with detailed asset data to enable initiatives such as:

1. IT cost reduction
2. Enterprise architecture
3. Cloud and data center migrations
4. Service management

Learn more about how to get started with ServiceNow CMDB sync.

Step 4 – Sync Externally Exposed Assets

Integrating with other sources, provides an outside-in perspective to detect assets exposed to the internet, marking known "managed" assets, discovering unknown assets, and facilitating security risk assessment. You can sync Externally Exposed Assets with the following methods:

- Shodan
- EASM - External attack surface management (An upgraded version of Shodan)

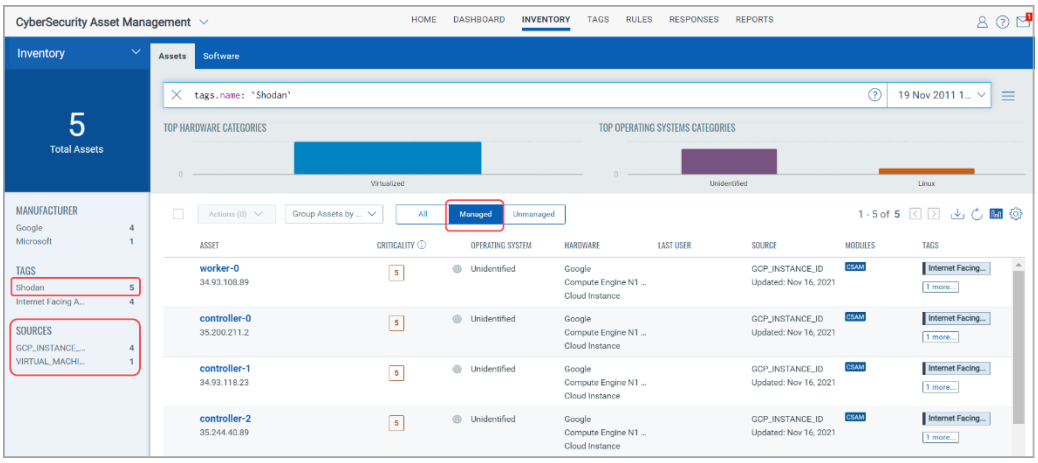
Shodan

With Shodan.io, you can:

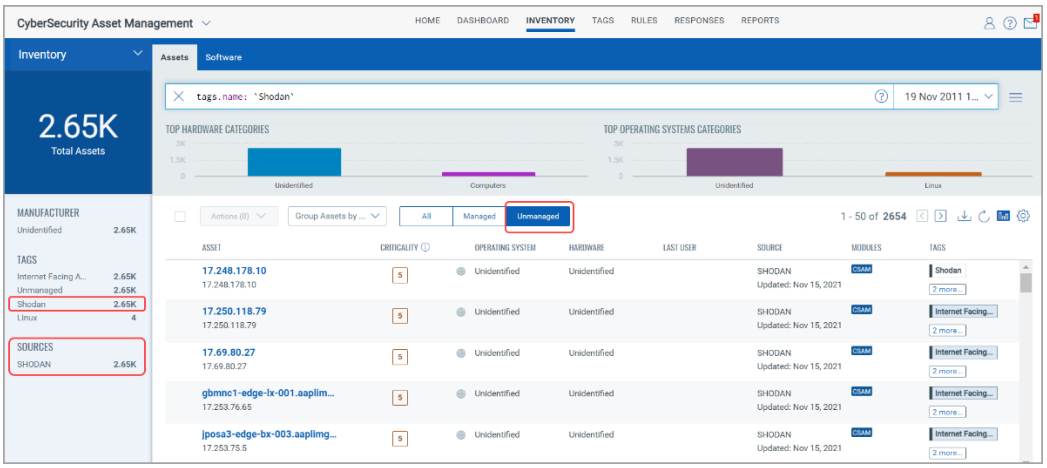
1. Access customer-specific public data from Shodan
2. Display it in the Asset Inventory and Asset Details
3. Create Unmanaged Assets to track newly identified endpoints.

Learn more about Synchronizing with Shodan to Get Attack Surface Visibility.

Managed Assets: The Shodan-imported assets that are currently in your inventory (detected through other Qualys inventory sources). These assets will have the "Shodan" tag visible. The inventory sources discovered by Qualys will serve as the source for the managed assets.



Unmanaged Assets: Assets imported from Shodan only. These assets will be displayed with 'Shodan' and 'Unmanaged' tag. Source for these assets will be 'SHODAN' in the inventory list.



Externally Attack Surface Management (EASM)- Beta

CSAM is nothing but a cloud service that allows customers to continuously discover, classify, remediate, and measurably improve their cybersecurity posture for internal and external IT assets. Right?

Wrong!

Qualys' unique approach to EASM is integrating the internal and external asset data from CyberSecurity Attack Management (CSAM) with its Vulnerability Management, Detection and Response (VMDR) solution into a single view. As a result, you can discover a greater number of undiscovered assets based on organization, domains, subdomains and immediately access and mitigate the cyber risk within the same workflow. And it also has more data compared to Shodan for the assets like

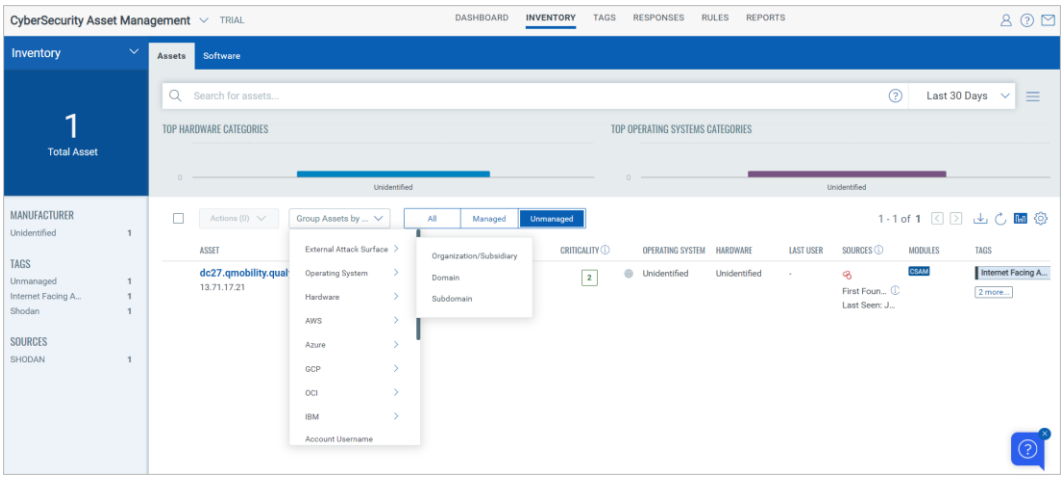
- DNS
- Domains
- Application stack
- Discovery path
- WHOIS information
- SSL

Qualys CSAM 2.0 offers you with a 'defense-in-depth' to update security posture with a full 360-degree coverage of the unknown assets.
You're now probably eager to discover about CSAM 2.0, as we are. So, lets jump on this bandwagon and find out the features of the newly added functionalities.

Inventory

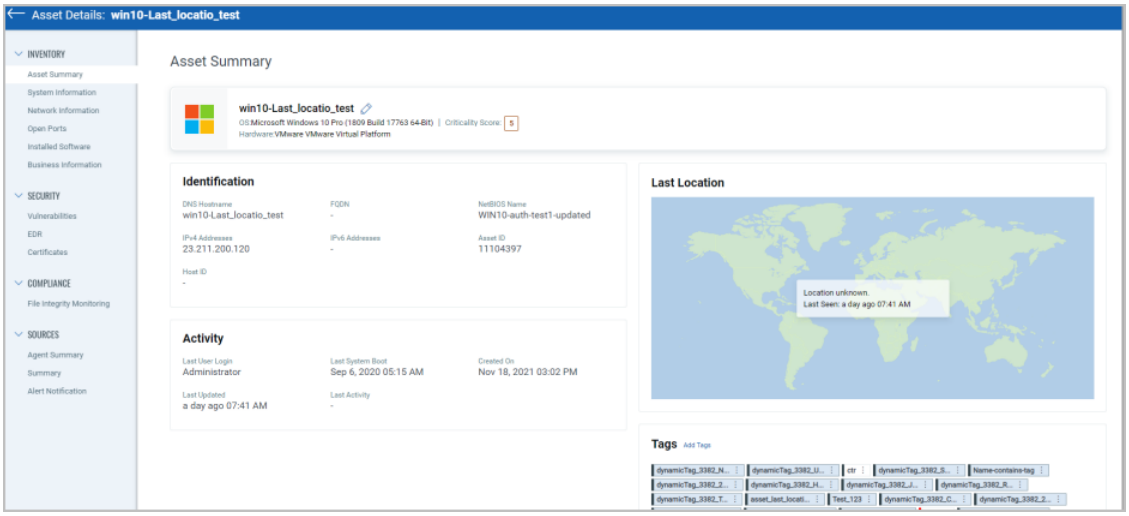
The Inventory tab provides you a consolidated view of assets and software in your organization. The Assets tab gives an overview of assets in your organization with summary of assets, consolidated list of assets, and a bar chart for top hardware and operating systems categories. The Software tab gives an overview of the software installed on the assets of your organization.

View Assets | View Software



Detailed asset information

View detailed asset information automatically, including the identify of an asset, its operating services, installed software, open ports, users, and more. This is a paid feature of CSAM.

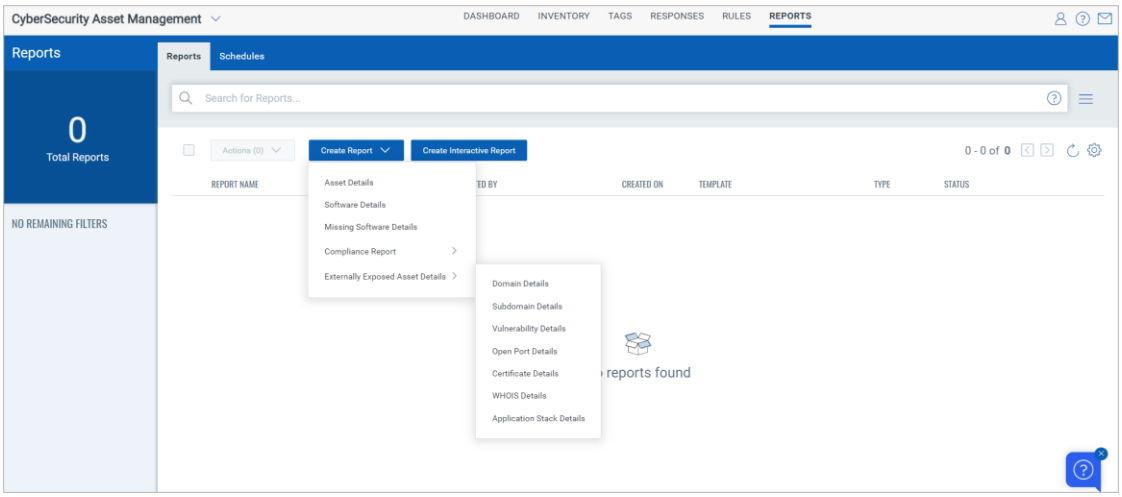


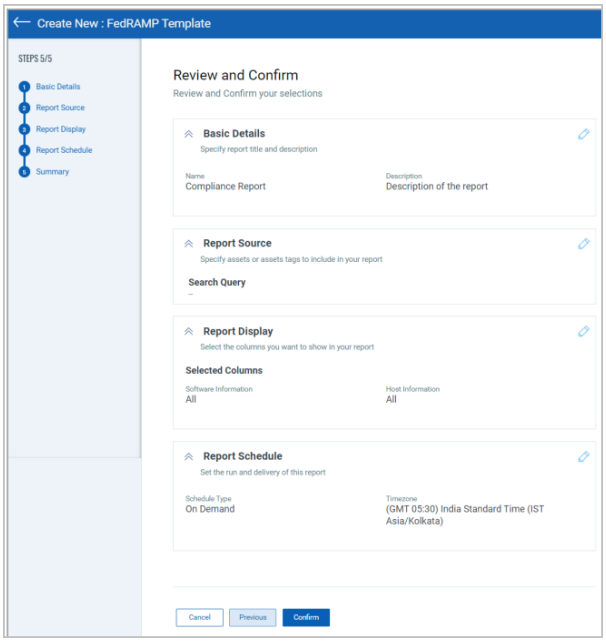
For more information, refer Configure Tags.

Reports

The CSAM 2.0 allows you to create curated reports including Externally Exposed Asset details like Domain details, Subdomain details, Vulnerability details, Open port Details, Certificate details, WHOIS details and Application Stack details to satisfy multiple regulatory requirements. This is a paid feature of CSAM.

Inside **Reports** tab > **Create Report** drop-down > Select the type of report as per the requirement.

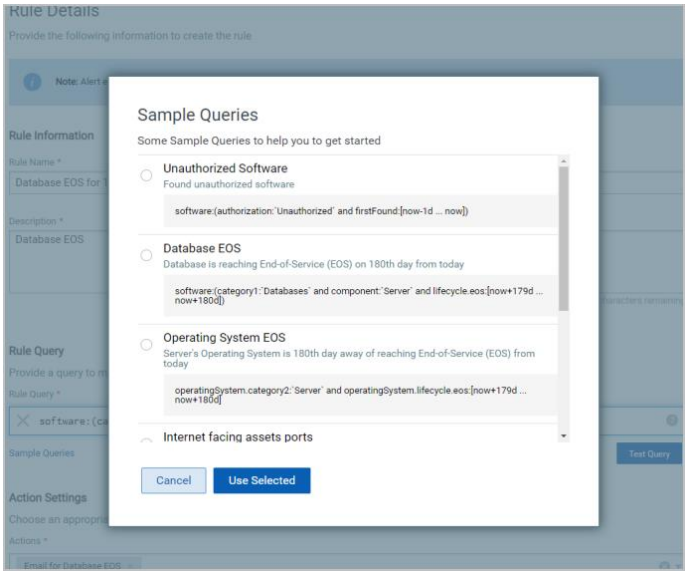




Rules

You can define and build list of Authorized and Unauthorized software and monitor the result.
You can create a rule to define software authorization (authorized, unauthorized, and needs review), activate the rule, and reorder the rule. Following sections help you to perform various steps to configure and execute the rule. This is a paid feature of CSAM.

Create authorization rule | Reorder authorization rule |Manage authorization rule



For more information, refer Configure Responses.

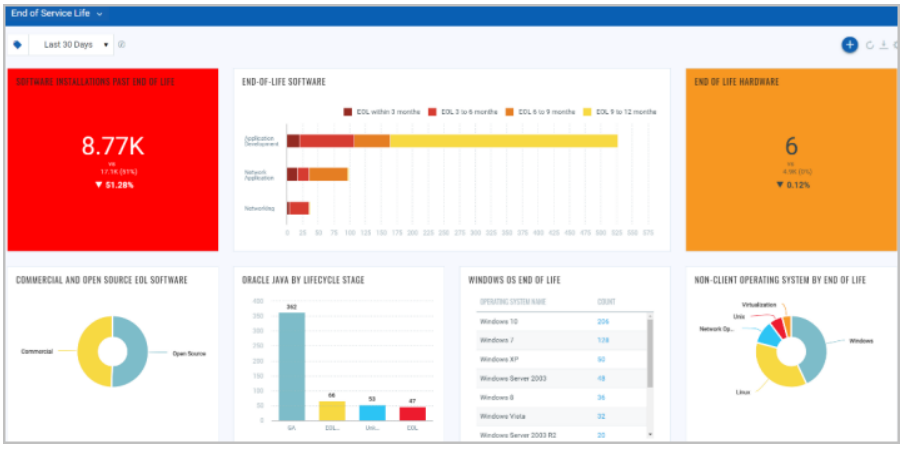
Tag Assets

You may organize the assets in your company by using asset tagging. Applying tags manually or setting up criteria for automatic asset classification into logical, hierarchical, business-contextual categories are also options. Tags are of two types: static and dynamic. A static tag will be generated by default. Tag Rules can be defined using dynamic tags. To assess a dynamic rule once it is generated or updated, tick the "Evaluate Rule on Creation" checkbox.

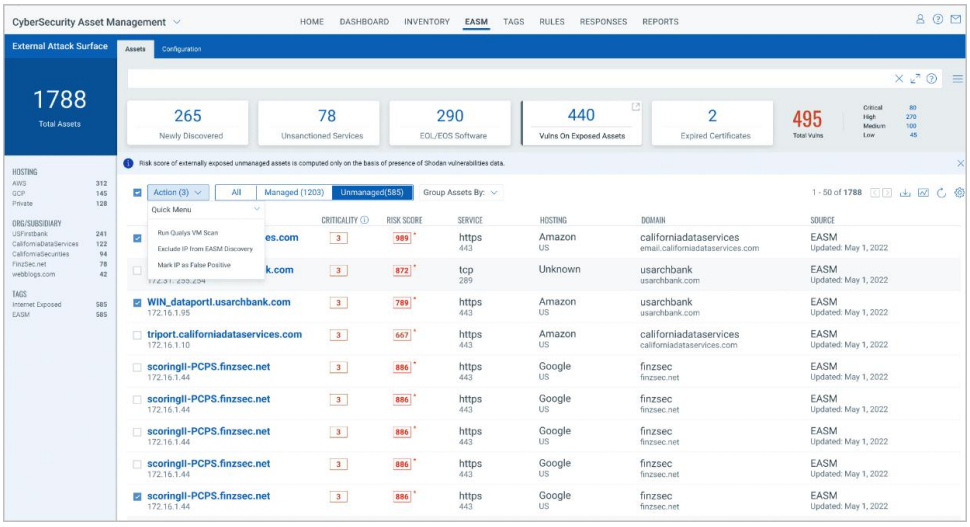
- Configure Tags
- Manage Asset Tags

Track Software, OS, and hardware product lifecycle information

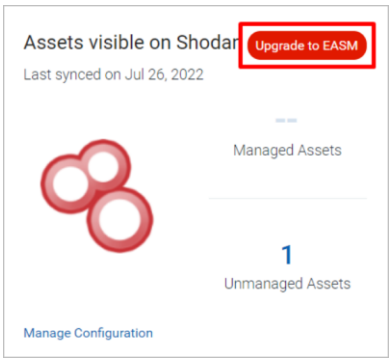
You may protect your environment using CSAM by getting rid of unsupported devices and applications. To discover assets that need replacing or upgrading, examine extensive information on the product lifecycles of hardware and software. Identifying licensable and open-source software will provide you more context. This is a paid feature of CSAM.

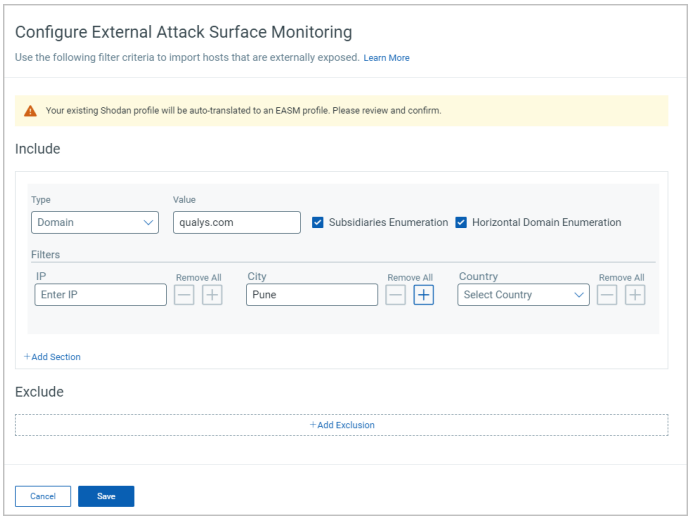


With CSAM 2.0, it's simple to begin identifying your external attack surface. All you have to do is check your root org or domain and activate the service. After that, the EASM service will start exploring for your internet-exposed assets.



Click the Upgrade to EASM on the Assets visible on Shodan card to view the Manage External Attack Surface Monitoring Configuration pop-up.





Once you have added/updated proper filter criteria, click **Save** to import assets in your inventory. Your sync will start within couple of hours. Once assets are imported, you'll see it on **Home** and **Inventory** tab.