Qualys

Vulnerability Management

Vulnerability Management Detection and Response (VMDR)

Overview of four applications **Asset Management**, **Vulnerability Management**, **Threat Protection**, and **Patch Management**. These applications are a part of VMDR

1. VMDR - Lab Tutorial Supplement
2. VMDR - Presentation Slides

Chart, diagram

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Diagram, radar chart

Description automatically generated

Chart

Description automatically generated with low confidence

Graphical user interface, text, application, email

Description automatically generated

Agents

The VMDR Welcome Page uses the Default VMDR Activation Key to download agents. It comes with **Asset Inventory (AI), Vulnerability Management (VM),** **Secure Configuration Assessment (SCA),** and **Patch Management (PM)** modules activated.

All Activation Keys include the **CyberSecurity Asset Management (CSAM**) application, by default.

Avoid including both the **Secure Configuration Assessment (SCA)**module and the **Policy** **Compliance (PC)** module in the same activation key. You can replace the SCA module with the PC module within one key. However, it is highly recommended that you create two separate keys for each of these modules.

Patch Management for VMDR

When Qualys PM is deployed as part of Qualys VMDR, you can build patch jobs that target specific vulnerabilities, vulnerability severity levels, and even vulnerabilities with known and existing threats. It automatically correlates, or matches discovered vulnerabilities with their required patches, so you can prioritize patches that fix your existing, high-risk vulnerabilities.

1 Correlates discovered vulnerabilities with their required patches automatically.

2 Leverages your existing Qualys Agents to deploy and uninstall patches.

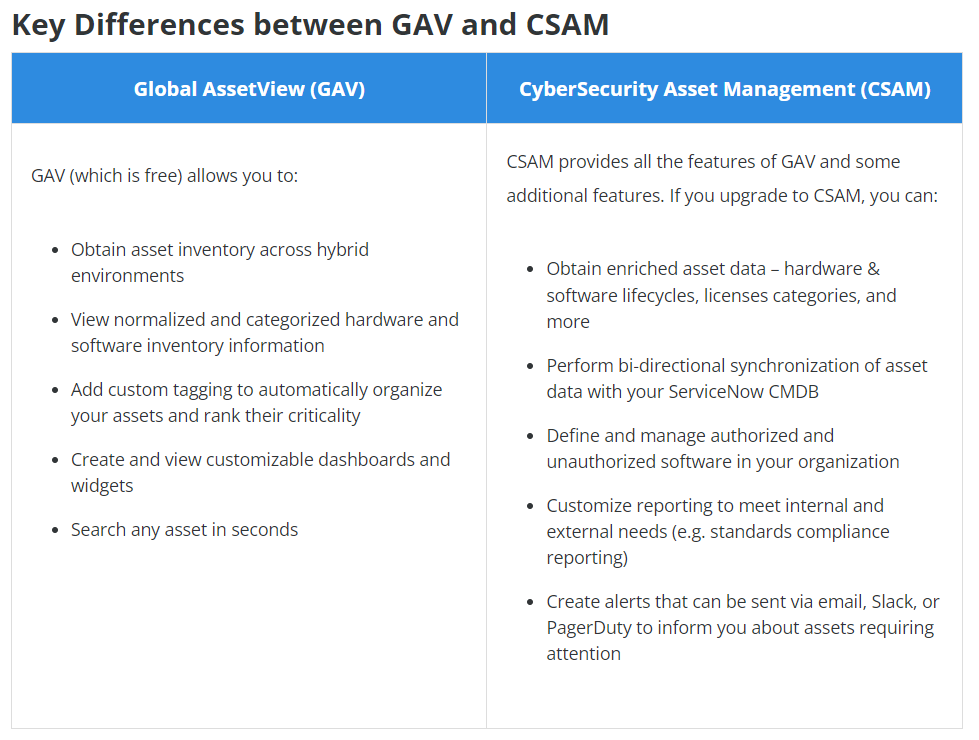
3 Covers OS and application patches, including patches from third-party software vendors (e.g., Adobe, Java, Google, Mozilla, Microsoft, etc...).

4 Provides patching just about anywhere an Internet connection is available (e.g., airports, coffee shops, remote offices, etc...).

5 Identifies missing and superseded patches.

6 Builds patch jobs that target specific vulnerabilities, severity levels, and known threats.

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



ServiceNow CMDB Integration

Qualys integration with ServiceNow (SN) CMDB helps security teams to gain comprehensive visibility into your IT asset inventory to immediately flag security and compliance risks.

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

Authorized & Unauthorized Software

**Need for Software Authorization**

Many organizations are driven by regulatory policies or other required compliance policies. This increases the need for a feature that defines authorized and unauthorized software lists and can implement such policies. Proactive tracking of unauthorized and authorized software is a crucial tool to reduce security risks and improve the health of your assets.

**CIS Control 2: Inventory and Control of Software Assets**

Center for Internet Security (CIS), Critical Security Control (CSC), Control 2 (CSC 2) are 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.”

To meet objective of CIS Control 2, CSAM provides three different types of software rules:

1. Authorized
2. Unauthorized
3. Needs Review

Reports

Other reports can be created using the Create Report dropdown menu. They include Asset, Software, and Compliance Reports. They are available in .csv file format.

* Asset Details - shows a detailed report of the selected assets based on host information (attributes)
* Software Details - shows a detailed report of the selected assets based on software and host information (attributes)
* Compliance Report - shows a detailed report of the assets for FedRAMP compliance based on software and host information (attributes)
* Missing Software Details – shows a detailed report of the selected assets based on missing software and host information (attributes)
* Externally Exposed Asset Details – shows a detailed report of the selected assets based on EASM details (domain, subdomain, vulnerabilities, open ports, certificate, whois, application stack)

