Qualys Ransomware Risk Assessment Playbook

January 2024

Table of Content

Introduction to Qualys Ransomware Risk Assessment Solution

Qualys.

Introduction to Qualys Risk Assessment Solution

To gain a foothold in an environment, attackers often exploit a known vulnerability. In many cases, organizations are unable to deal with such initial breaches in a timely manner. Also, ransomware players use the same techniques against different organizations to exploit ransomware-related vulnerabilities. As a result of not patching those vulnerabilities - even after being exploited - ransomware players will exploit the same vulnerability against the same organization running a new ransomware campaign!

Qualys Ransomware Risk Prevention Solution helps organizations operationalize government guidelines, providing a specific ransomware heatmap to shrink their attack surface and eliminate risk areas. It features a dynamic dashboard for risk management, aligns with CISA's cybersecurity requirements, and uses extensive research to offer a proactive, actionable plan against ransomware threats.

Read the Blog about Qualys Ransomware Solution

Strategies for Protecting Your Business from Ransomware Attacks

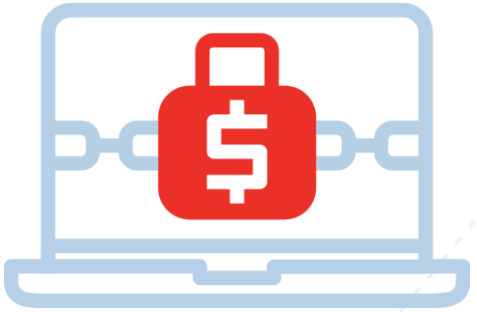
Refer to Qualys Documentation and Qualys Videos to set up and configure Qualys capabilities, as required.

Qualys.

What I Get with Ransomware Solution (RAS) Enabled

When the Ransomware (RAS) is enabled, you can:

- Identify and prioritize ransomware vulnerabilities in line with CISA guidelines in your interactive **3 Tips For Ransomware Prevention** dashboard.
- Get prioritized, actionable insights for missing patches required to remediate your prioritized ransomware vulnerabilities.
- Deploy prioritized patches, utilizing automation wherever applicable. Ensure out-of-the-box support for internet-facing applications, including browsers, readers, and more, via the Qualys Patch Management application.



Qualys.

What will I see in my subscription?

You will start seeing the following in your subscription based on your customer type:

Existing Customers

- After you import the dashboard in the Unified Dashboard module, the new dashboard will be available in your library for your ransomware risk assessment and remediation. Data based on agents that are enabled for the campaign is displayed in the widgets.
- Best Practice Controls for Malware/Ransomware Prevention policy in Policy Compliance.
- (Only if you have CSAM enabled in your subscription) Default authorization rules, 'Software Elevating Cybersecurity Risk for Data Center Assets' or 'Most Common Ransomware Attack Vectors' to receive alerts on potential threats. Configure Authorization Rule.

New Customers

You will import the dashboard in the Unified Dashboard module, which will be provisioned in your subscription, along with other Qualys modules. The new dashboard will be available in your library for your ransomware risk assessment and remediation. Data based on agents that are enabled for the campaign is displayed in the widgets.

Trail Users

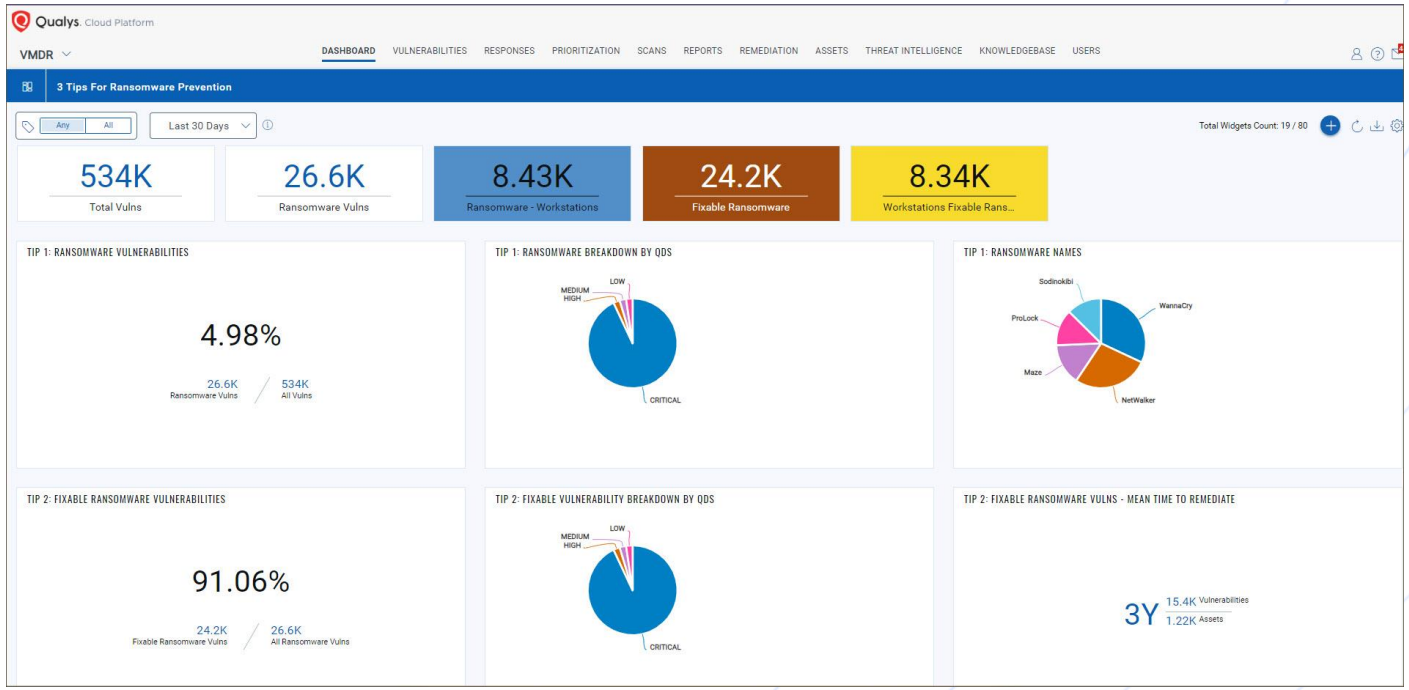
Once the trial is enabled, you can start using the Qualys Cloud capabilities provisioned in your subscription immediately to start assessing and mitigating your ransomware risk exposure. For more information, you can contact your TAM.

Qualys.

About the Ransomware Prevention Dashboard

Qualys enables organizations to quickly identify and locate vulnerabilities in their infrastructure.

The **3 Tips For Ransomware Prevention** dashboard displays the most critical vulnerabilities that are commonly exploited by ransomware groups. Ransomware vulnerabilities are automatically prioritized by Qualys Detection Score (QDS). This allows organizations to quickly identify and address critical ransomware vulnerabilities before they become problematic. The dashboard also allows you to patch vulnerabilities with a single click, if you have the Patch Management module enabled in your subscription.



Security leaders need this dashboard to ANALYZE the security posture of their infrastructure and what actions they can take to PREVENT a ransomware attack.

Qualys.

Advantages of using this dashboard

You can use this dashboard to:

Track	• Overall potential true risk based on our "TruRisk Score" • Vulnerabilities in VMDR based on Ransomware RTIs • Ransomware-related vulnerabilities, which are automatically prioritized by Qualys Detection Score (QDS) • Vulnerabilities that can be patched
Patch	• Patch based on Ransomware RTI. You can use our Patch Management module or leverage your existing tools • Patching on assets that operate software for processing internet data, such as web browsers, browser plugins, and document readers • 3rd party apps - focused on web browsers and Adobe reader • Create RTI-based automated patch jobs via our Patch Management module

With Trending enabled for dashboard widgets, you can keep track of vulnerability trends and ransomware-related compliance controls in your environment.

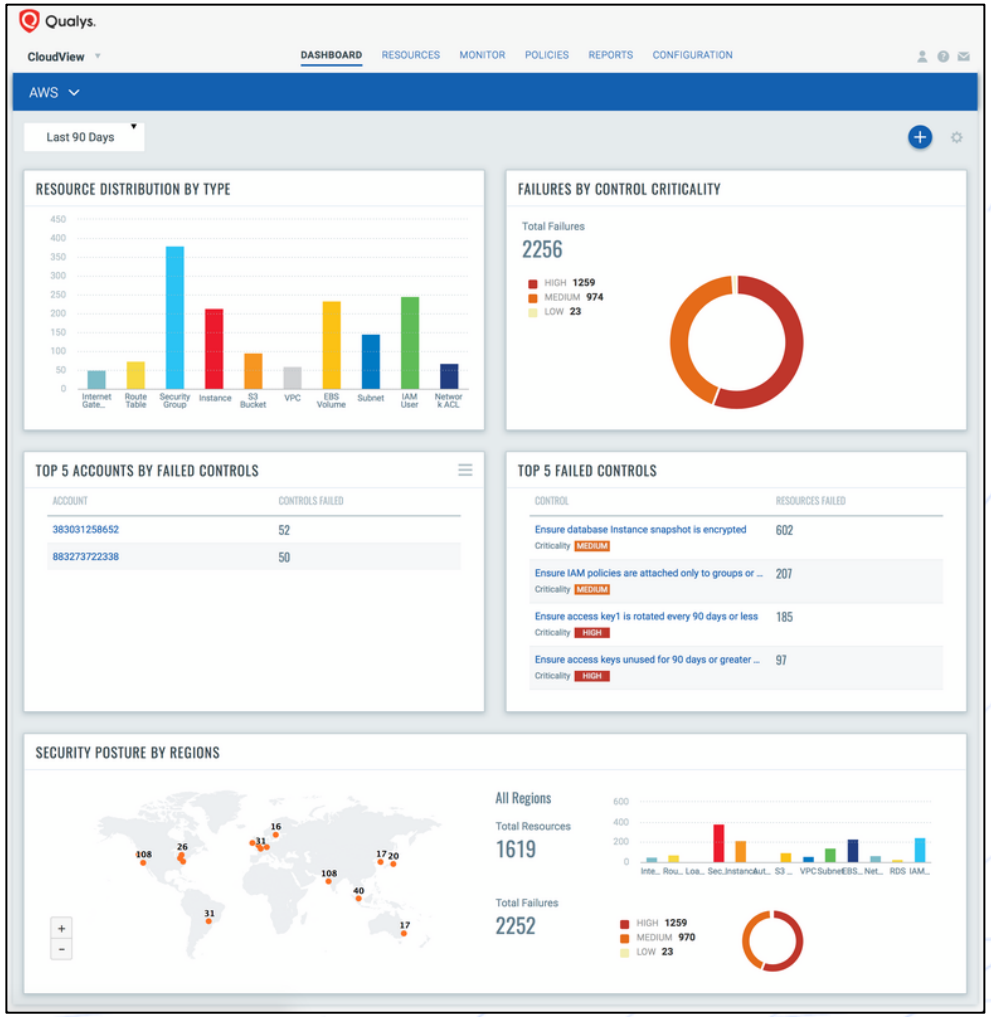
Qualys.

How do I access the dashboard?

Your subscription does not include this dashboard by default.

To access this dashboard

1. Click here to download the JSON file. If you need any help, you can reach out to your TAM.
2. Import the JSON file into the Unified Dashboard module.
3. Open the **3 Tips For Ransomware Prevention** dashboard in the **Dashboard** tab.



Note: Qualys Patch Management or a similar patch management tool is required for patching vulnerabilities.

Qualys.

How do I view the dashboard?

To view the Ransomware Prevention Dashboard

In the **Dashboard** tab, click the **Dashboard Picker** and then select the dashboard. The dashboard is added to your list of available dashboards, and you can start viewing ransomware-related data in your widgets.

Qualys.

Let’s Get Started

The most important step to start protecting your organization from ransomware threats is having an extensive, thorough, and up-to-date inventory.

With an in-depth IT asset inventory, you can:

- Identify dangerous blind spots in advance
- Adequately understand your environment to prioritize assets and risks
- Plan further visibility and protective measures.

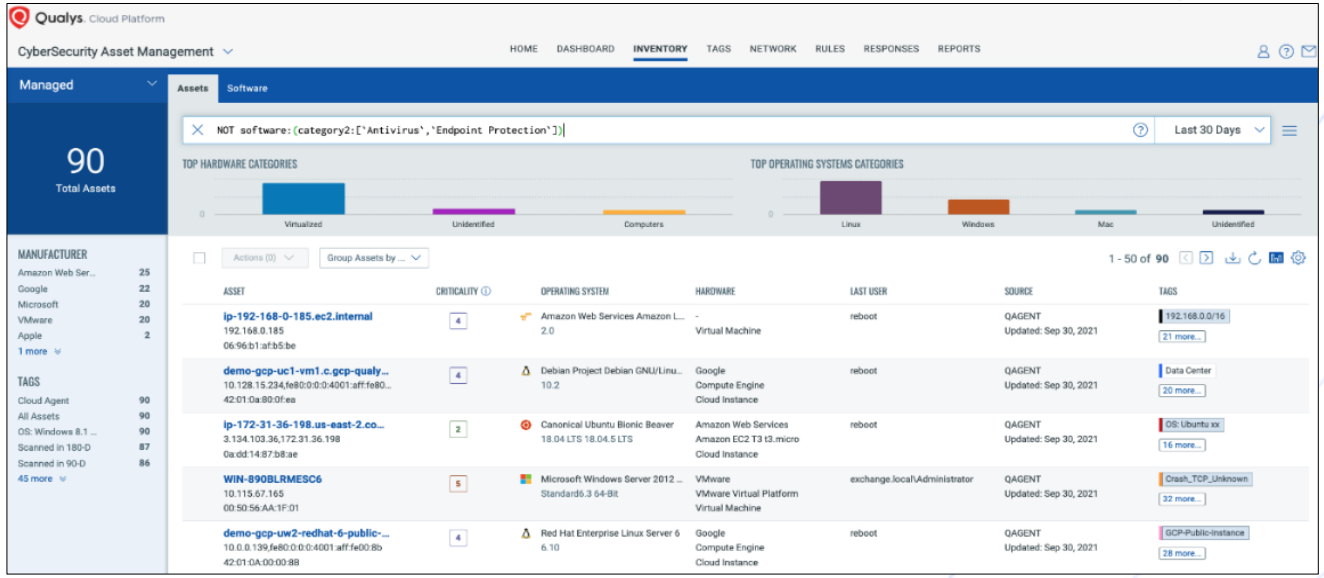
Qualys.

Step 1 – Build your Inventory

CyberSecurity Asset Management (CSAM) helps you discover and inventory assets and accurately assess complex IT infrastructure so you can quickly identify and remediate risk.

Note: This step is for customers with CSAM enabled in their subscription. You can contact your TAM to enable CSAM for your subscription.

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 ransomware threats right away.



[Install Qualys Cloud Agents](#) | [Cloud Agent Getting Started Guide](#) | [Cloud Agent Onboarding Videos](#)

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

[CSAM Quick Start Guide](#) | [CSAM Onboarding Videos](#) | [CSAM Online Help](#)

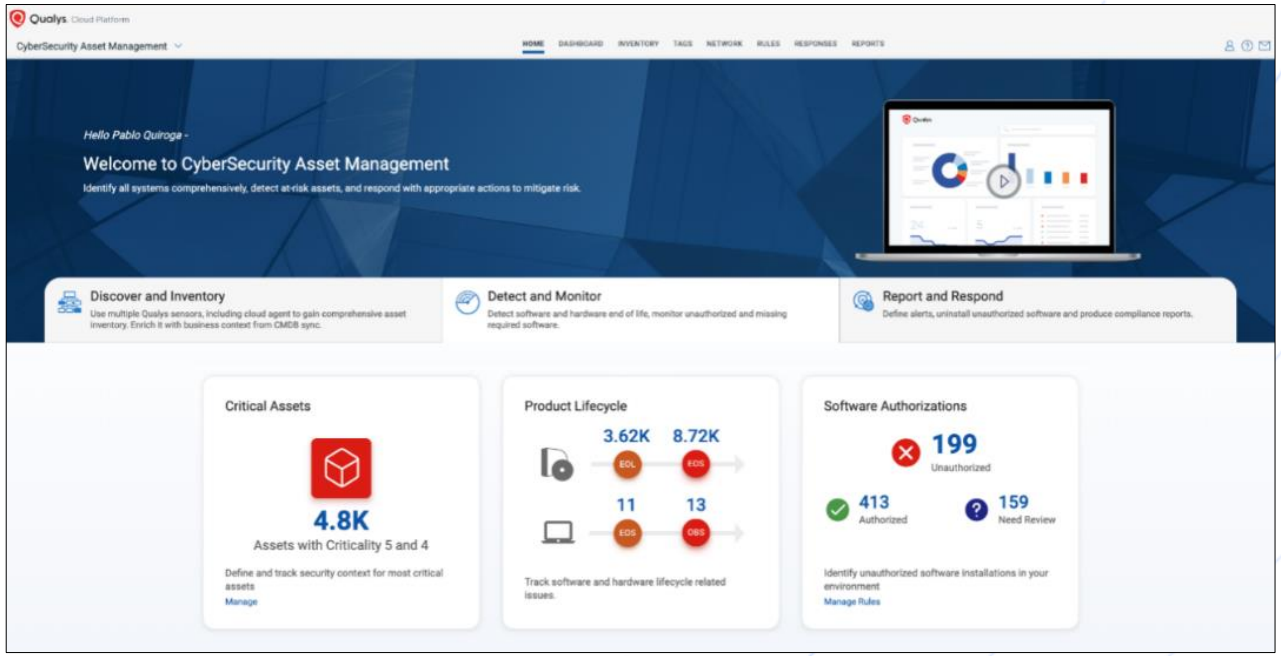
Qualys.

Step 2 (a) – Detect at-risk Assets and Applications

CSAM enriches your asset inventory with in-context, relevant information to help you detect at-risk assets and applications. You can identify and set alerts for assets that are running unauthorized software or are not using anti-virus/endpoint security tools.

Unauthorized software should be removed to quickly reduce unnecessary attack vectors. With CSAM, you can easily define rules to monitor unauthorized software installations.

Use CSAM to identify assets that are missing required security software, such as Antivirus and Endpoint Protection. Navigate to the Inventory tab and form queries to search for desired results.



[CSAM Quick Start Guide](#) | [CSAM Onboarding Videos](#) | [CSAM Online Help](#)

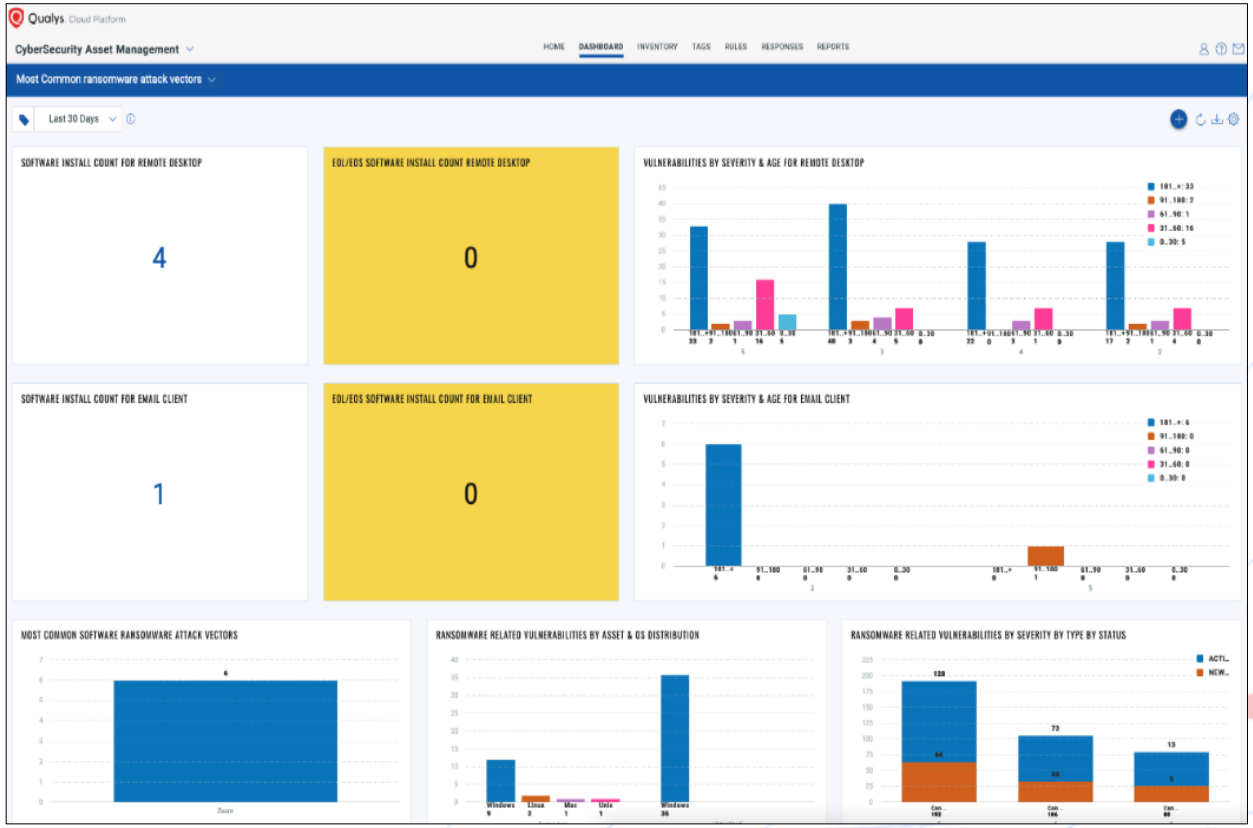
Qualys.

Step 2 (b) – Detect at-risk Assets and Applications

You can also identify End-Of-Life/End-Of-Support software, which can be used as ransomware attack vectors. End-of-Support software is one of the first things hackers look to exploit because they are aware that the publishers are no longer providing security updates and patches.

Configure tags so you can apply them to assets in your subscription. This helps you to organize your assets and to manage user access to them. Let's say you create a tag "RDP Asset" to find all assets with Remote Desktop Protocol (RDP) service enabled, then all assets with RDP service enabled will be grouped along with any new hosts that get added to the environment.
[How to configure tags?]

Example of CSAM Ransomware Dashboard

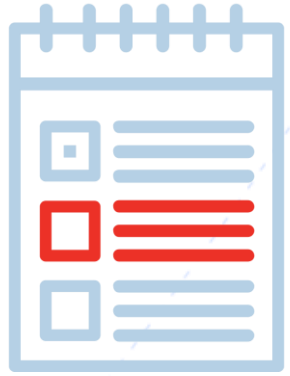


Step 2 (c) – Detect at-risk Assets and Applications

Configure Authorization Rules

Configure rules to monitor critical events that satisfy the conditions specified in a rule and send you alert messages if events/incidents matching the conditions are detected.

You can enable the default authorization rules, ‘Software Elevating Cybersecurity Risk for Data Center Assets’ or ‘Most Common Ransomware Attack Vectors’, to receive alerts on potential threats.



Navigate to **Rules > Software Rules** and choose a rule. Then, from the **Quick Actions** menu, click **Enable**.

You can also create your own rules. Know more about Creating Software Rules.

Go back

Qualys.

Step 3 (a) – Prioritize Vulnerabilities

Now that your inventory is in place use VMDR to assess, prioritize, and remediate the vulnerabilities and misconfigurations on your assets.

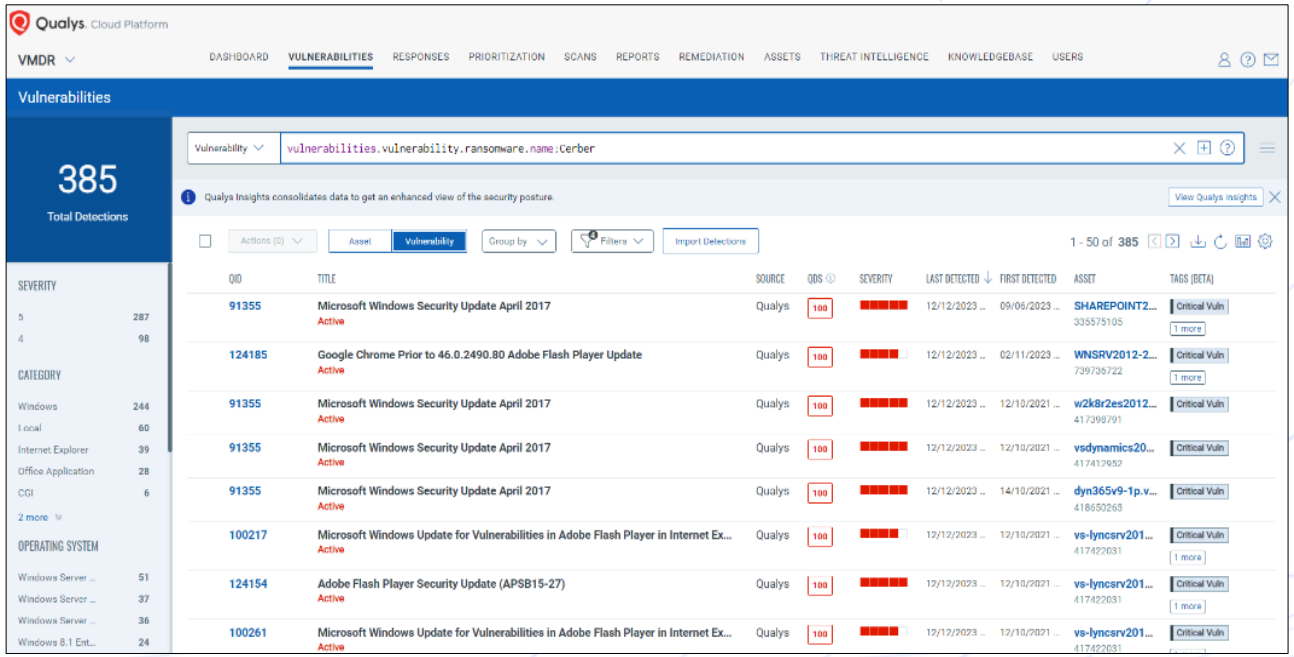
VMDR helps you automatically detect and prioritize the specially researched vulnerabilities, and the threat feed helps you understand your asset exposure to high-profile exploited vulnerabilities.

Navigate to VMDR and use the tags to identify and analyze the vulnerability information of your ransomware-scoped assets. We will prioritize the risk against specially researched CVEs and generate a report.

Now that hosts with the “RDP” service are identified by the tag you created; you want to detect which of these assets have flagged this vulnerability. VMDR automatically detects new vulnerabilities like Windows RDP, Exchange Server vulnerability, and more based on the updated Knowledgebase.

You can see all your impacted hosts for this vulnerability tagged with the ‘Ransomware asset tag in the vulnerabilities view by using this QQL query:

vulnerabilities.vulnerability.ransomware.name:Cerber



VMDR Onboarding Videos | VMDR Getting Started Guide | VMDR Online Help

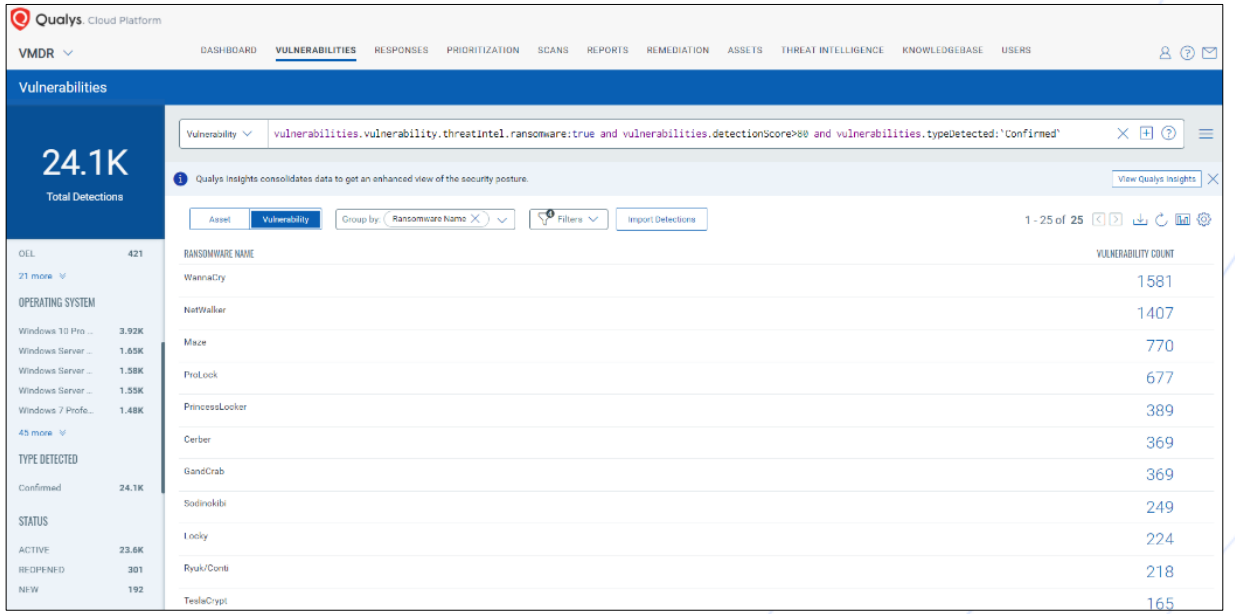
Step 3 (b) – Prioritize Vulnerabilities

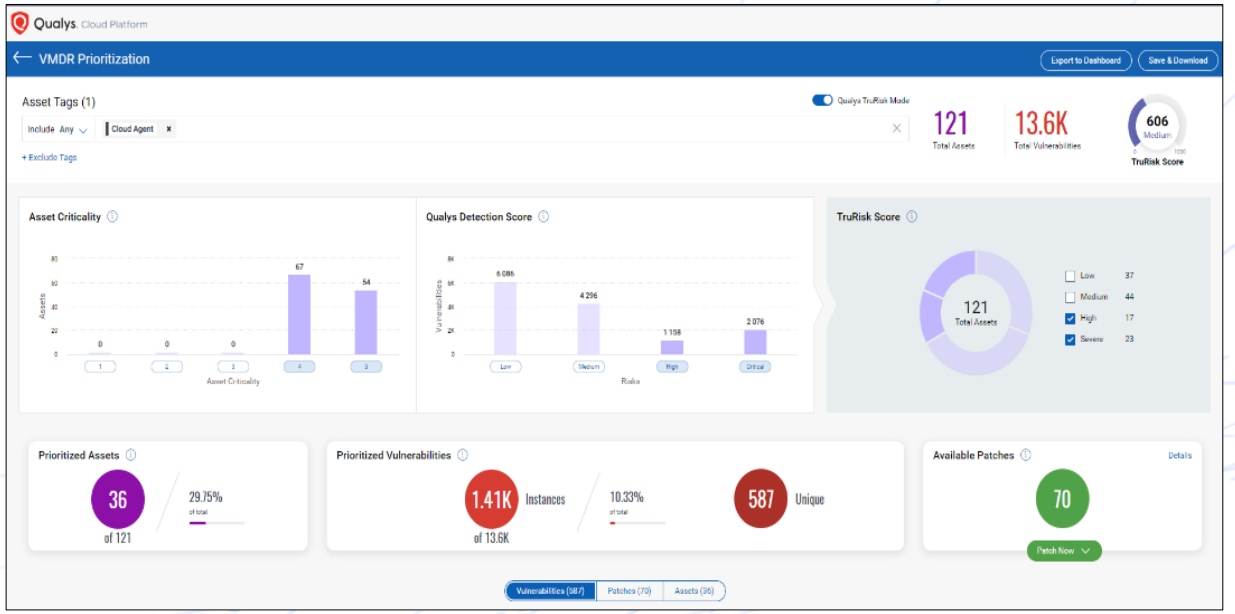
From a prioritization perspective, TruRisk scores can be further combined with additional attributes using QQL to refine the prioritization process. Here's an example:

> Vulnerabilities.vulnerabilities.threatIntel.ransomware:true and vulnerabilities.detectionScore>80 and vulnerabilities.typeDetected:'Confirmed'

Generate a VMDR Prioritization Report to detect which vulnerabilities to remediate first, identify the most critical threats, and prioritize patching.

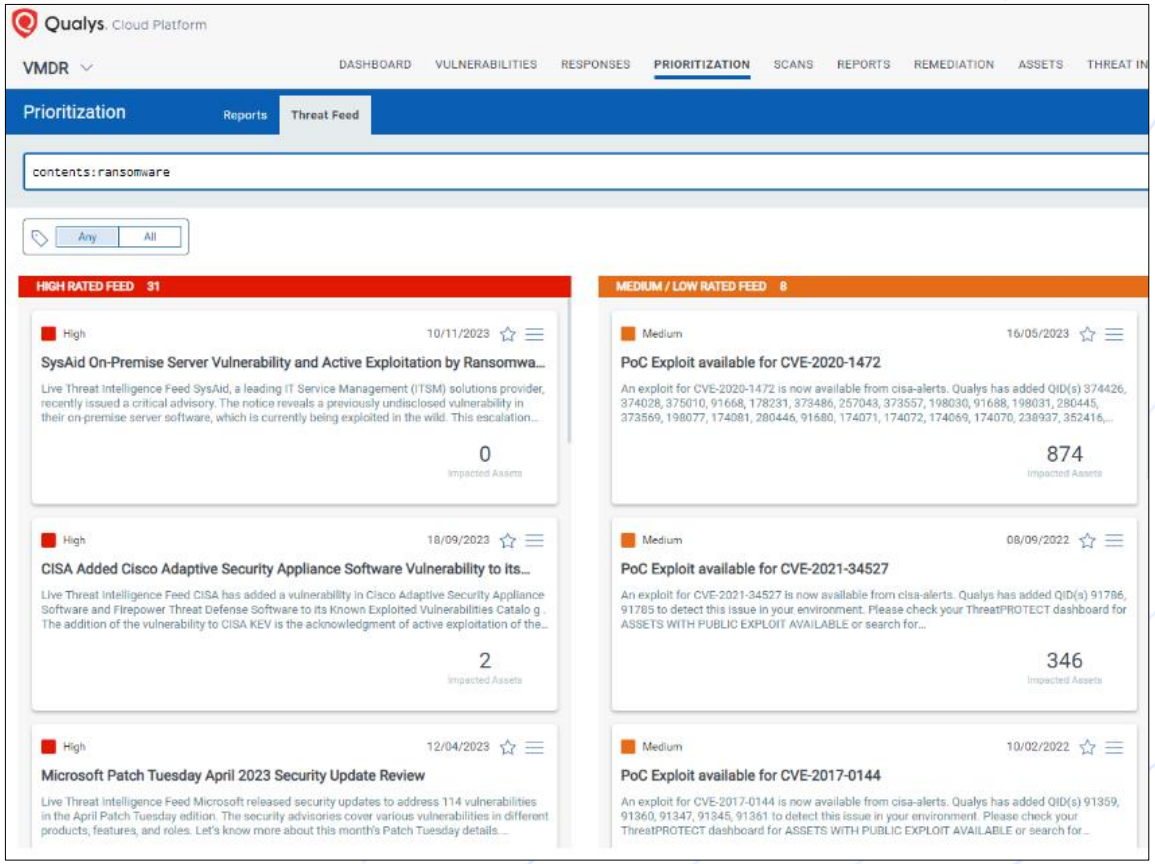
Using the prioritization report, the ransomware vulnerabilities can be easily prioritized using "Ransomware" Real-Time Threat Intelligence.





Step 3 (c) – Prioritize Vulnerabilities

VMDR also enables you to stay on top of these threats proactively via the ‘live threat feed’ provided for threat prioritization. With the ‘live feed’ updated for all emerging high and medium risks, you can clearly see the impacted hosts against threats. Simply click on the impacted assets for the “Ransomware” feeds to see the vulnerability and impacted host details.



[Introduction to VMDR Videos](#) | [Best Scanning Strategy Videos](#)

Read more about the vulnerability threat landscape here:

[An In-Depth Look at the Latest Vulnerability Threat Landscape](#)

[An In-Depth Look at the Latest Vulnerability Threat Landscape (Attackers’ Edition)](#)

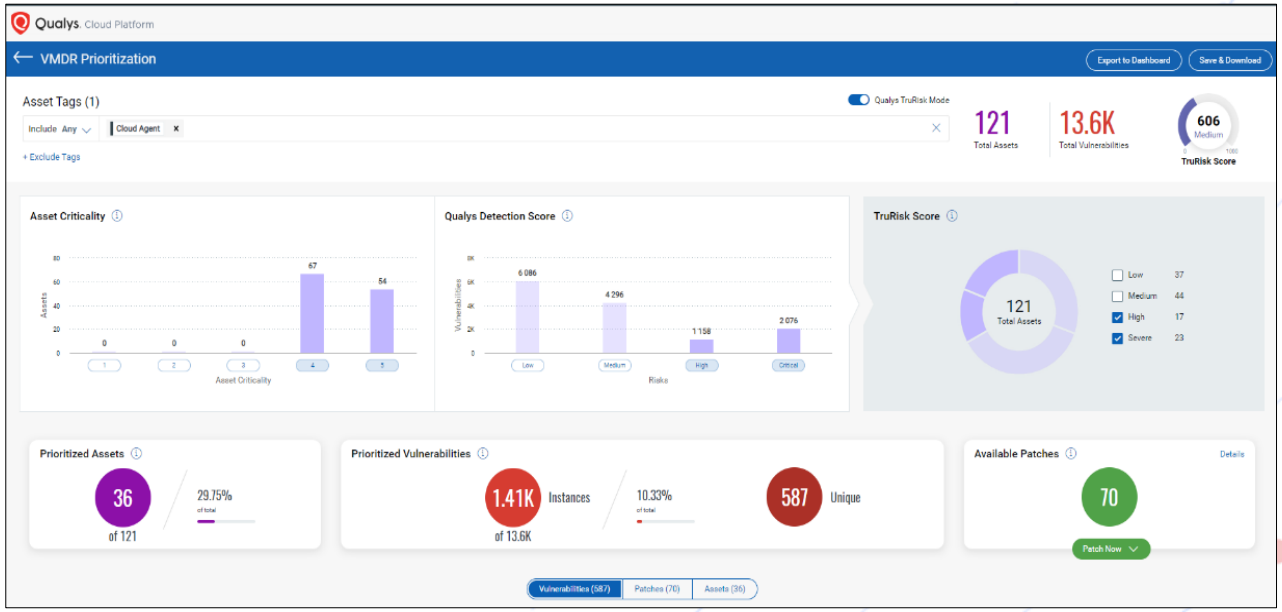
Qualys.

Step 4 – Deploy Patches

Ensure that all assets, system components, and software are protected from known vulnerabilities by deploying curated ransomware patches.

You may also use our zero-touch patching capability to intelligently identify and automatically deploy the proper patches required for remediating vulnerabilities.

You can quickly identify all missing patches from your VMDR prioritization report. Use the method described above to filter only ransomware-related vulnerabilities. Select the vulnerabilities you would like to remediate and add them to a new job. Qualys will automatically map all the selected vulnerabilities to the patches that remediate those vulnerabilities and are relevant to your environment. Only the latest patches will be included, saving the need to deploy old patches that have been superseded. Configure the patch job and deploy the patches to your vulnerable assets.



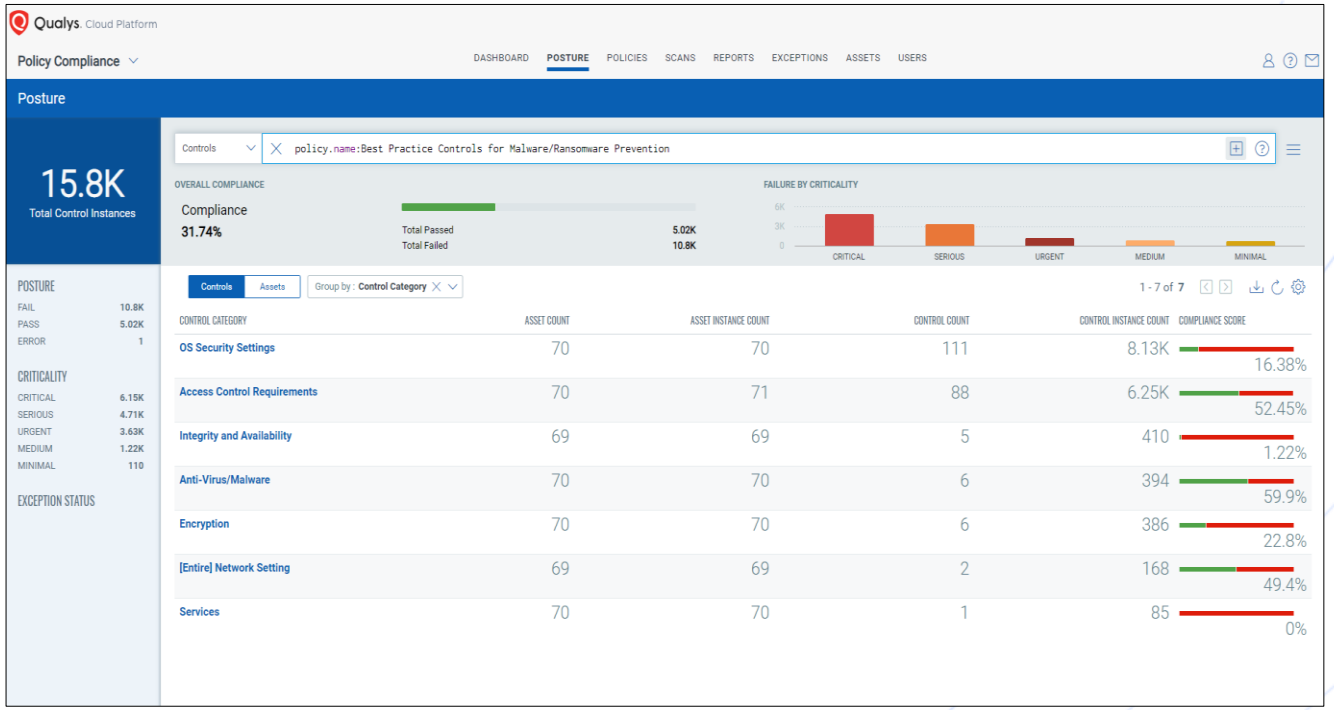
[Deploying Patch Jobs on Assets](#) | [Patch Management Getting Started Guide](#) | [Patch Management Videos](#)

Qualys.

Assess Misconfigurations

The Policy Compliance (PC) and Security Configuration Assessment (SCA) help organizations evaluate research-driven configuration policies for ransomware to identify, assess and remediate misconfigurations exploited by ransomware. Configuration management adds context to your overall vulnerability management.

Qualys Policy Compliance provides Best Practice Controls for Malware/Ransomware Prevention policy that contains the critical controls mapped to MITRE ATT&CK mitigations and tactics recommended by CISA.



Navigate to the **Policy Compliance > Dashboard > Posture** tab in your subscription to view all findings returned from the policy.

Security Configuration Assessment Online Help | Policy Compliance Getting Started Guide | Policy Compliance Videos

Qualys.