Qualys Endpoint Detection and Response v2.x

Release Notes

Version 2.3

February 28, 2023

Here's what's new in Endpoint Detection and Response 2.3!

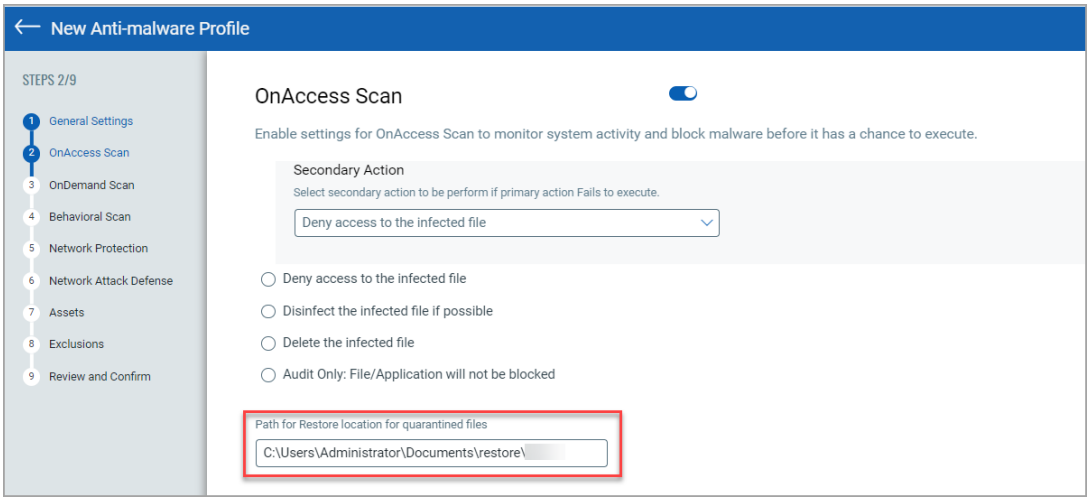
What's New

Endpoint Detection and Response 2.3 brings you some improvements and updates!

Added New Field in OnAccess Scan Page of Anti-Malware Profile

With this release, we have added a new field **Path for Restore location for quarantined files.** This is an optional field and can be accessed from the **Configuration** tab. In this field you can provide the path where you want the quarantined files to be restored. Perform the following steps to restore the quarantine file:

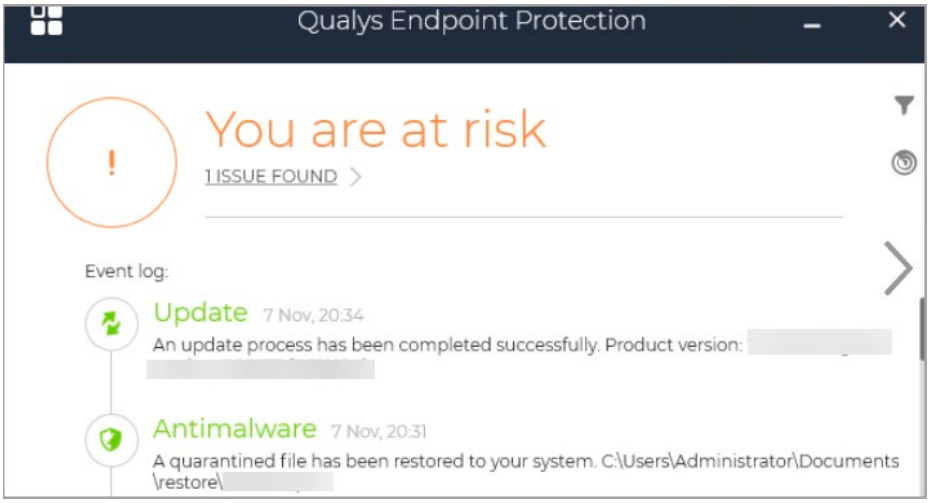
1. From the **Configuration** tab, click **Anti-Malware Profile**.
2. Click **New Anti-malware Profile**.
3. In the **OnAccess Scan** page, provide the **Path for Restore location for quarantined files**.



4. Provide the information for other pages as per your organization's requirement.
5. Click **Create Anti-malware Profile**. For more information about creating anti-malware profile, see EDR Online Help.

Note: The custom restore location path is used when the original location of the file cannot be restored. Hence, it is recommended to set the custom restore location path that is available in the system. The custom restore path should be excluded from File Exclusions. For more information about File Exclusion, see EDR Online Help.

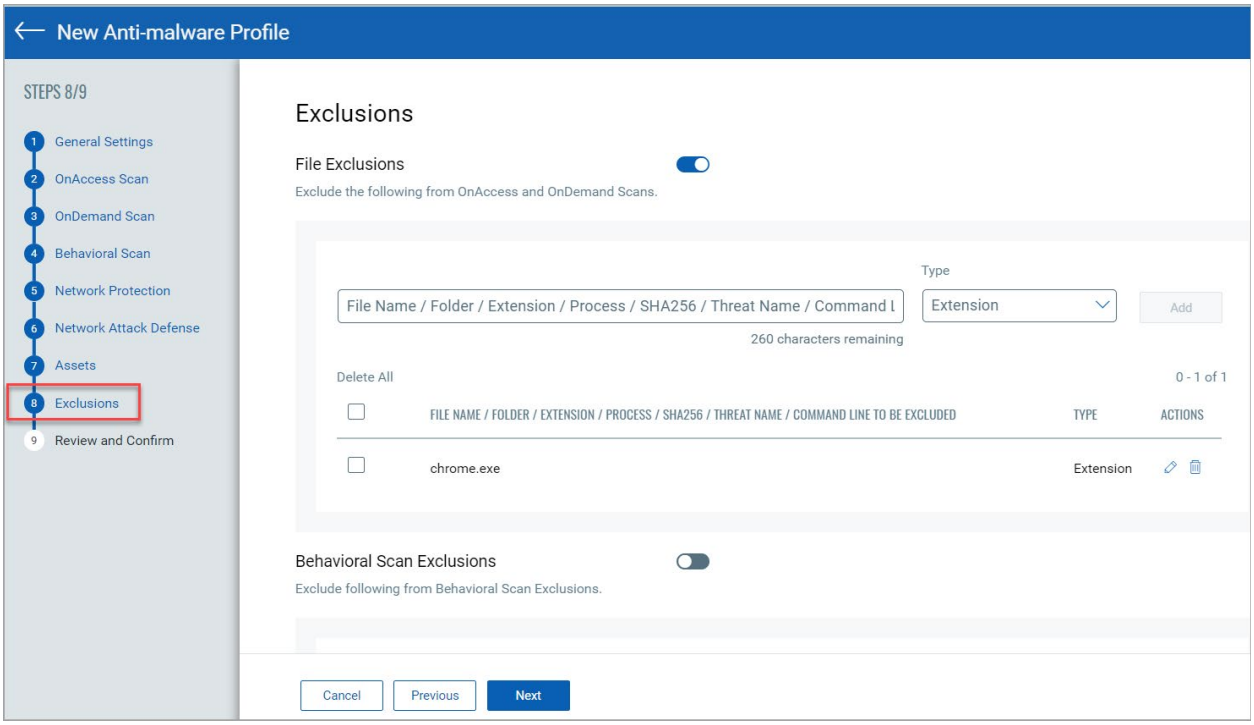
Following screenshot is an example of the notification:



Added Exclusion Type in Exclusions Page of Anti-Malware Profile

With this release, we have defined the type of exclusions that you can include while creating a new Anti-malware profile or for an existing profile. The inputs for **File Exclusions**, **Behavioral Scan Exclusions**, **Traffic Scan Exclusions**, and **Anti-Phishing Exclusions** are listed in **Configuration** tab under **Anti-Malware Profile** tab. Toggle the exclusion type to exclude the type from the scan. For more information about Exclusion Support, see EDR Online Help.

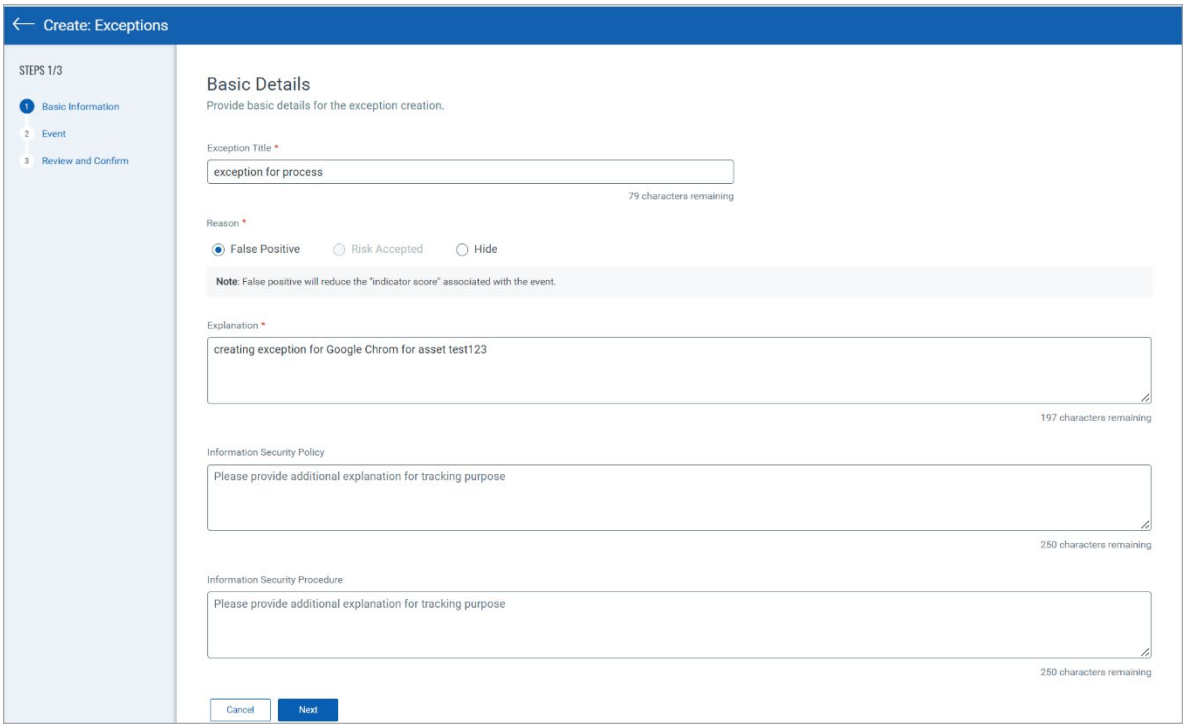
Following screenshot is an example of File Exclusions:



Added Create Exception Option in Quick Actions Menu of Hunting Tab

We have introduced the **Create Exception** option that allows you to suppress a past or a future event that you consider is non-malicious. This option is available in the **Quick Actions** menu and can be performed for an event listed in **Historic View** or **Current View**. While creating an exception, you need to choose the **Reason** among the following Reason option categories:

- **False Positive**: It reduces the indicator score associated with the event that is 8 or greater than 8.
- **Risk Accepted**: It reduces the indicator score associated with the event that is between 1 to 7.
- **Hide**: If you do not want to change the score for False Positive or Risk Accepted you can choose this option to hide the event. Events from the **Current View** tab is moved to the **Exempted Events** tab.

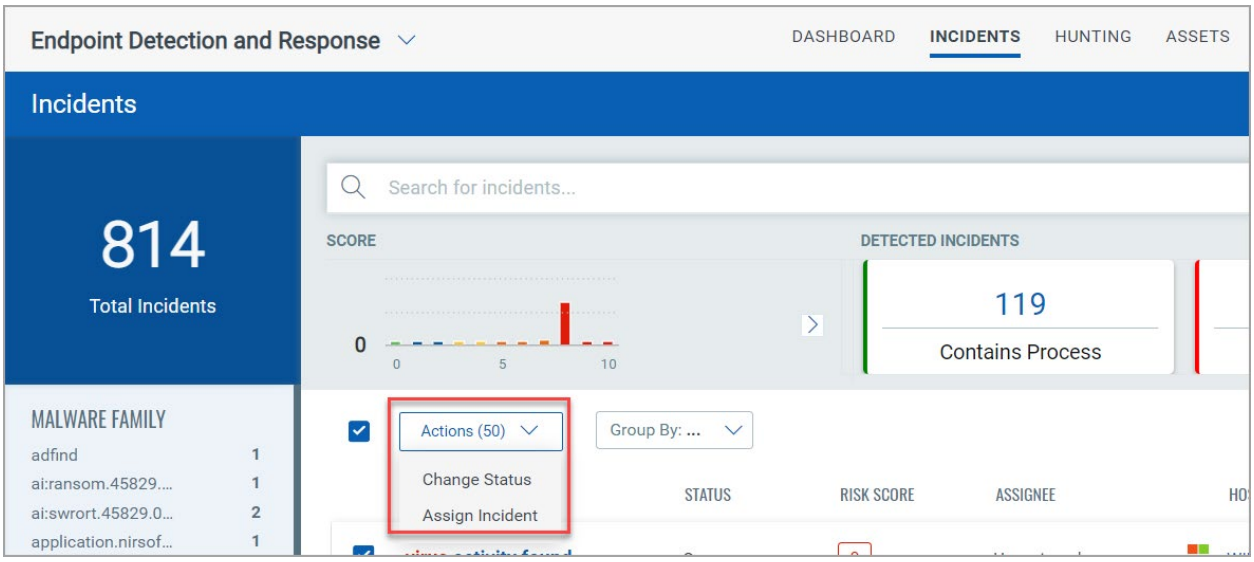


For details on steps to Create Exception, see EDR Online Help.

Enhanced Incident Workflow

We have enhanced incident workflow by introducing **Change Status** and **Assign Incident** as the two new options. You can perform bulk actions of **Change Status** and **Assign Incident** using the **Actions** drop-down menu. The bulk actions cannot be performed if the Assignee is different.

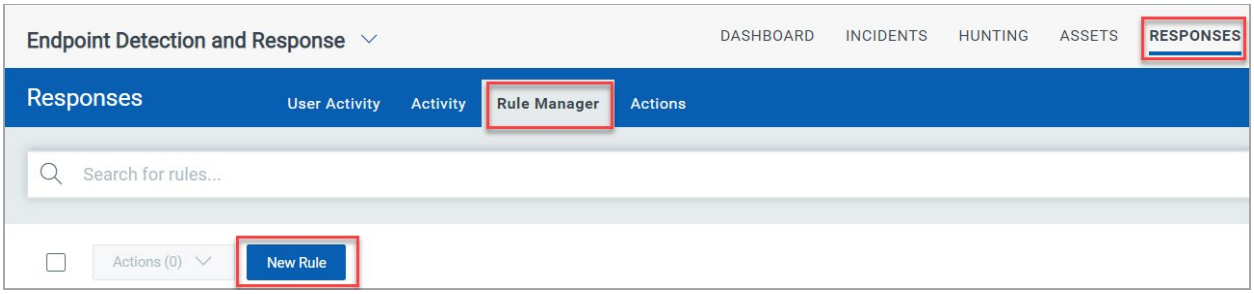
- **Change Status**: The status of an event can be – Open, In Progress, Closed, and Re-open. By default, the status of an event is **Open**.
- **Assign Incident**: An incident can be assigned to the user using the Assign Incident option. By default, the assignee is displayed as **Unassigned**.



After the status is changed or an incident is assigned, the updated changes are listed in the **Incidents** tab. For more information on how to change the status and assign incidents, see EDR Online Help.

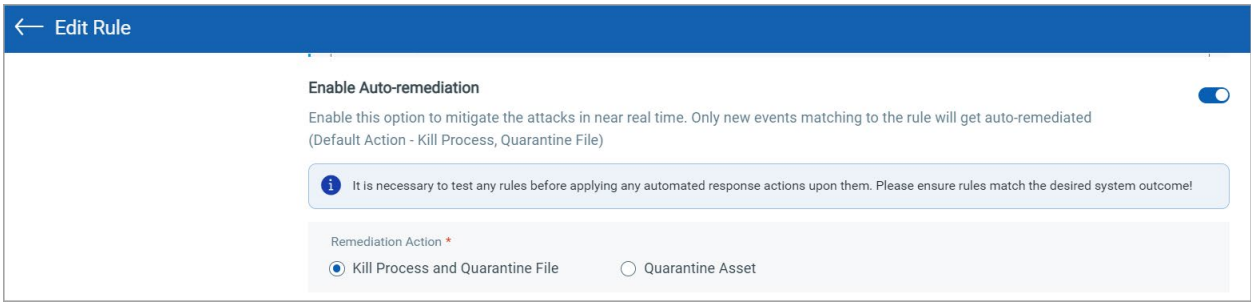
Introduced Auto-Remediation of an Event

With this release, we have introduced a feature that auto-remediates an event. You can auto-remediate an event by setting a rule from the **Responses** tab.

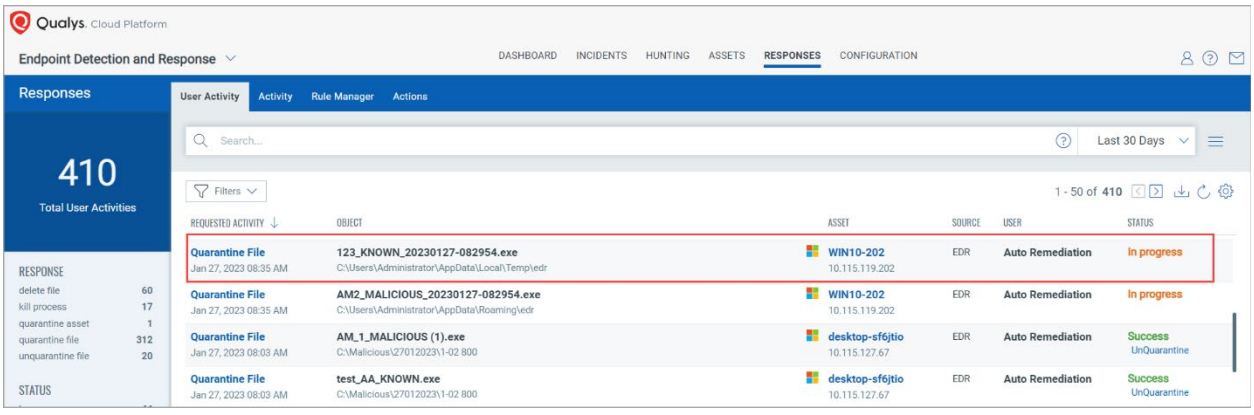


Auto-remediation can be done for the following:

- Kill Process and Quarantine file
- Quarantine Asset



After the changes are saved the quarantined action is automatically triggered. Following screenshot is an example:



To perform the Auto-remediation step-by-step, see EDR Online Help.

Introduced New Tokens

- **assets.tags.name**: This token uses the string value to list the assets with the tag name.
- **incident.status**: This token uses the string value to list the incident status.
- **incident.assignee**: This token uses the string value to list the assignees.

For more information about these tokens, see EDR Online Help.