



# Qualys Endpoint Detection and Response v1.x

## Release Notes

Version EDR 1.0

September 21, 2020

Here is what you get with Qualys EDR 1.0!

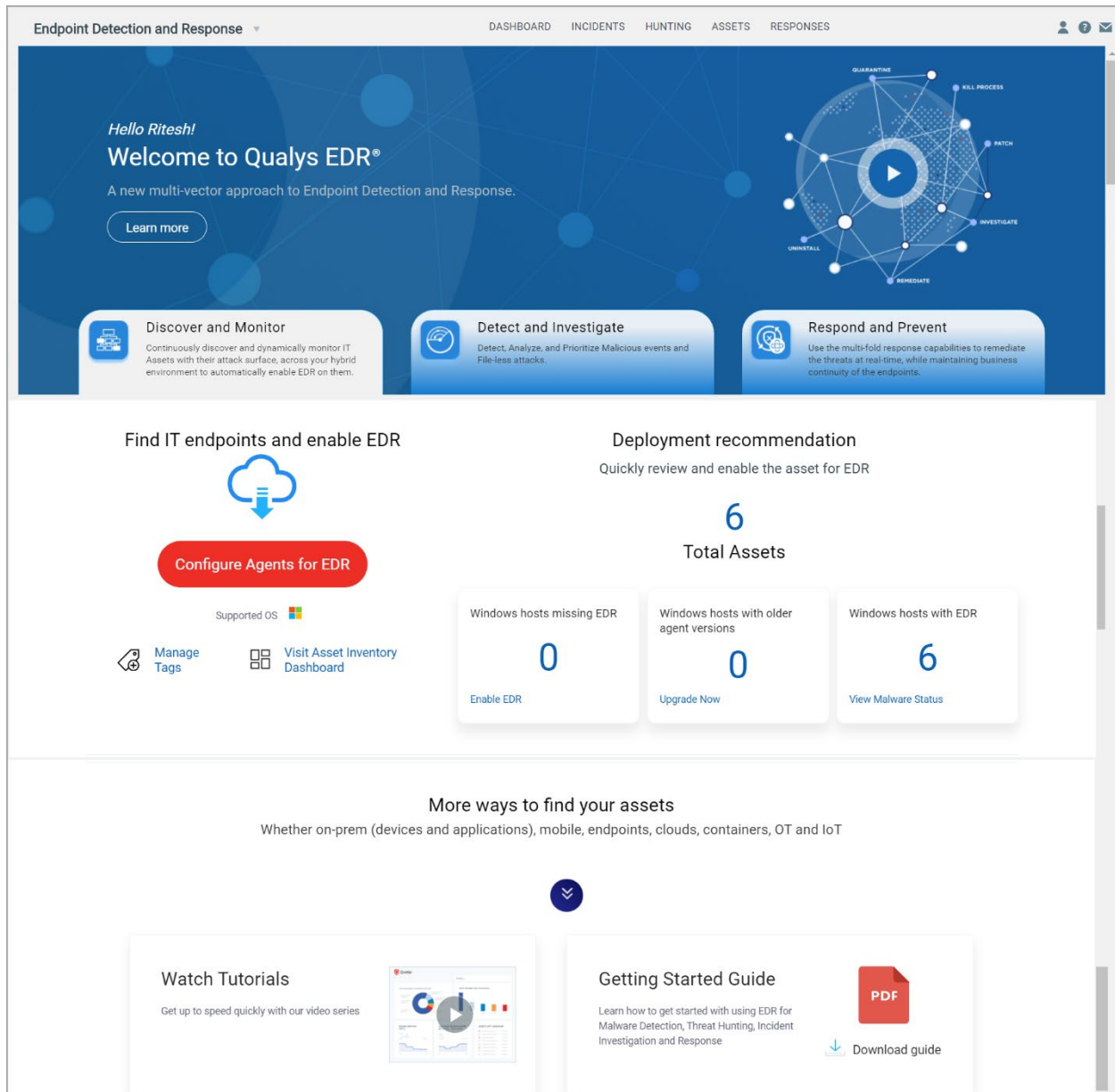
- [New EDR Welcome Page](#)
- [Download and Configure Cloud Agent from Welcome Page](#)
- [Unified Dashboard \(UD\) Support for EDR](#)
- [View Events Tree](#)
- [View Hunting Tab](#)
- [View Events Detail Page](#)
- [New Tokens](#)

Click [here](#) to see the EDR Beta Release Notes!

## New EDR Welcome Page

With this release, we have redesigned the Welcome page.

This page helps you get started in a few quick steps, gives you a quick overview of what you'll get with EDR, and information on the high-level workflow of EDR. We also give on-screen guided assistance to help you get started.



The screenshot displays the Qualys EDR Welcome Page. At the top, a navigation bar includes 'Endpoint Detection and Response' and tabs for 'DASHBOARD', 'INCIDENTS', 'HUNTING', 'ASSETS', and 'RESPONSES'. The main header area features a personalized greeting 'Hello Ritesh!', the title 'Welcome to Qualys EDR®', and a subtitle 'A new multi-vector approach to Endpoint Detection and Response.' with a 'Learn more' button. To the right is a circular diagram illustrating the EDR workflow: QUARANTINE, KILL PROCESS, PATCH, INVESTIGATE, REMEDIATE, and UNINSTALL. Below this are three primary action cards: 'Discover and Monitor' (continuously discover and dynamically monitor IT Assets), 'Detect and Investigate' (Detect, Analyze, and Prioritize Malicious events and File-less attacks), and 'Respond and Prevent' (Use the multi-fold response capabilities to remediate the threats at real-time, while maintaining business continuity of the endpoints).

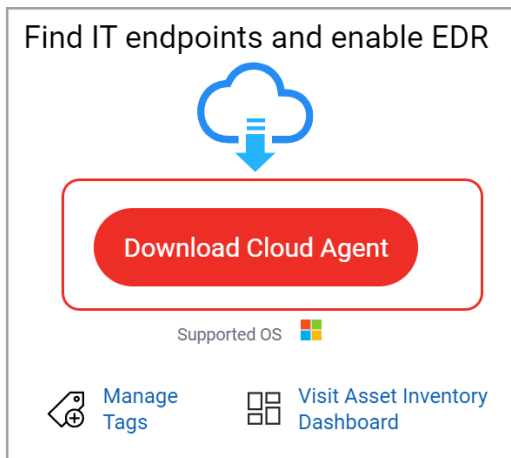
The middle section is divided into two main areas. On the left, 'Find IT endpoints and enable EDR' features a cloud icon and a red button 'Configure Agents for EDR'. Below this are links for 'Manage Tags' and 'Visit Asset Inventory Dashboard'. On the right, 'Deployment recommendation' prompts users to 'Quickly review and enable the asset for EDR'. It shows a total of 6 assets and three categories: 'Windows hosts missing EDR' (0, with an 'Enable EDR' link), 'Windows hosts with older agent versions' (0, with an 'Upgrade Now' link), and 'Windows hosts with EDR' (6, with a 'View Malware Status' link).

The bottom section, 'More ways to find your assets', states 'Whether on-prem (devices and applications), mobile, endpoints, clouds, containers, OT and IoT'. It includes a dropdown arrow and two resource cards: 'Watch Tutorials' (with a video player thumbnail and the text 'Get up to speed quickly with our video series') and 'Getting Started Guide' (with a PDF icon, the text 'Learn how to get started with using EDR for Malware Detection, Threat Hunting, Incident Investigation and Response', and a 'Download guide' link).

## Download and Configure Cloud Agent from Welcome Page

We now give you the option to download and configure Cloud Agent for EDR from the Welcome page. You'll need to install a Cloud Agent that's been activated for EDR on each asset you want to monitor for suspicious activity.

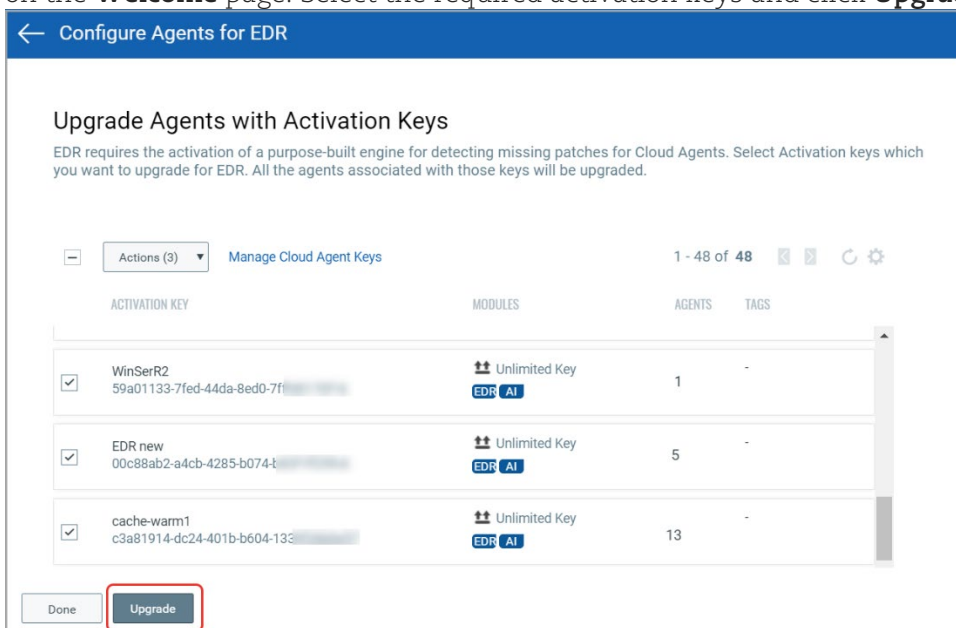
If you are a new customer, you must first download and install the default EDR key. To download key, click **Download Cloud Agent** under the **Discover and Monitor** tab on the **Welcome** page.



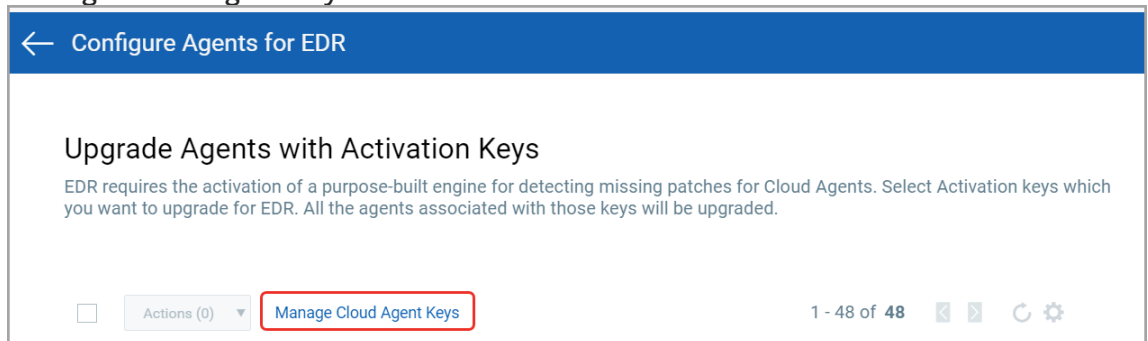
Note: You must upgrade to Cloud Agent version 4.1 and above to utilize all the EDR functionality.

If you are an existing customer, you can either:

- Select the existing activation key and upgrade the associated agents for EDR. To enable the existing agents, click **Configure Agents for EDR** under the **Discover and Monitor** tab on the **Welcome** page. Select the required activation keys and click **Upgrade**.



- Install new Cloud Agent and activate the agent for EDR. To install a new Cloud Agent, from the **Welcome** page, click **Discover and Monitor** > **Configure Agents for EDR** > **Manage Cloud Agent Keys**.



For detailed procedure for all the above options, see **Download and Configure Cloud Agent for EDR** topic from the Online help or Getting Started Guide.

## Unified Dashboard (UD) Support for EDR

Dashboards help you visualize your assets, see your threat exposure, leverage saved searches, and remediate priority of malicious/suspicious events quickly.

We have integrated Unified Dashboard (UD) with EDR. UD brings information from all Qualys applications into a single place for visualization. UD provides a powerful new dashboarding framework along with platform service that will be consumed and used by all other products to enhance the existing dashboard capabilities.

You can use the default EDR dashboard provided by Qualys or easily configure widgets to pull information from other modules/applications and add them to your dashboard. You can also add as many dashboards as you like to customize your detection and remediation view.

Click the Add Widget icon on the Dashboard page to go to customize your dashboard.

The screenshot displays the 'Add Widget to Dashboard (EDR)' interface. On the left, a sidebar lists templates under the heading 'TEMPLATES':

Template	Count
Asset View	9
Certificate View	10
Container Security	15
CloudView	12
EDR	9
Global IT Asset Inventory	17
Patch Management	9
Threat Protection	17
Vulnerability Management	6

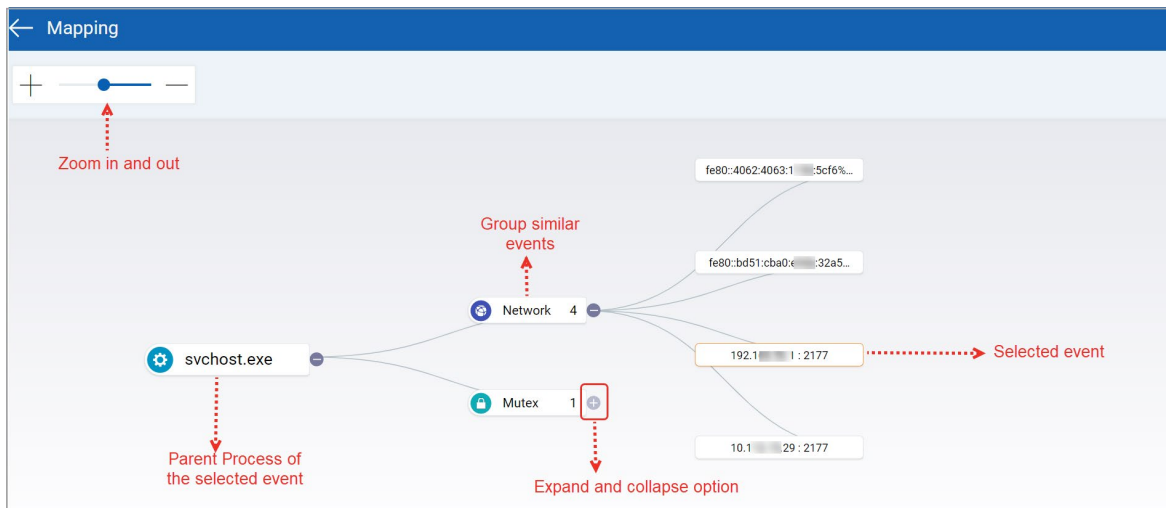
The main area features a blue header with a back arrow and the title 'Add Widget to Dashboard (EDR)'. Below the header, there is a search bar and a 'Create Widget' button. The main content area is divided into sections:

- EDR EDR**: A section with a search bar and a 'Create Widget' button. Below this, it says 'Select the template you would like to customize or add to your dashboard'.
- All Widgets (9)**: A section with tabs for 'All Widgets (9)', 'Default Widgets (4)', and 'User-defined Widgets (1)'. It lists two widgets:
  - ASSET AND MALWARE SUMMARY**: Displays details of infected assets and malware. It has an 'Add To dashboard' button.
  - DEFAULT WIDGET**: Trying system widget. It has a 'Customize Widget' button.

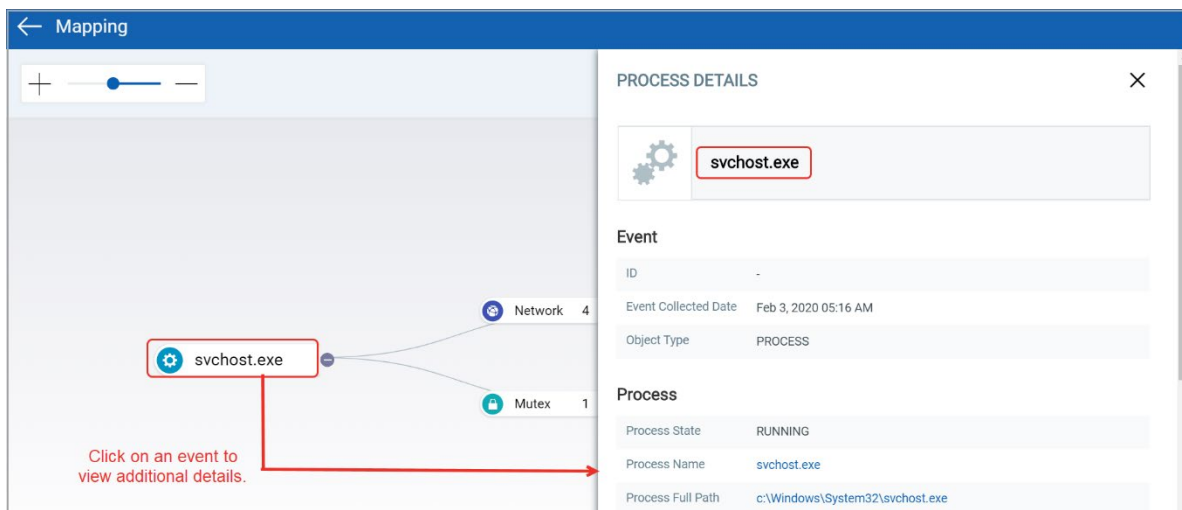
## View Events Tree

For better usability, we have added the following changes to the Events Tree:

- The selected event is now marked with an orange border.
- To help you identify the type of event in a hierarchy view, we have now grouped similar events under an event type and added an icon for the event type.
- You can use the expand (+) and collapse (-) option to navigate through the nodes.



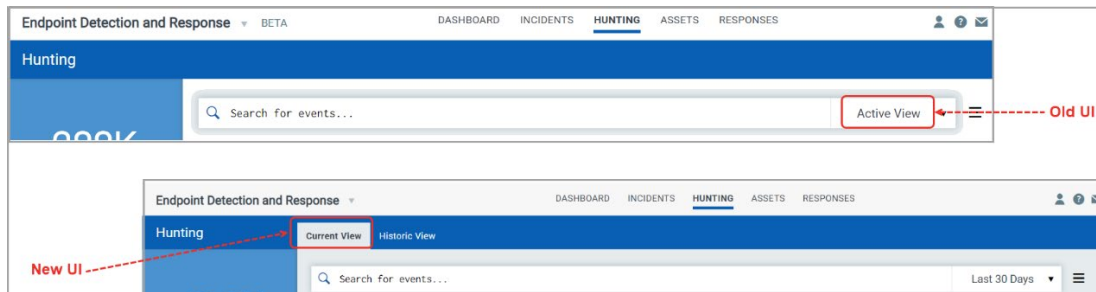
- You can click on the event to view additional information about an event.



## View Hunting Tab

For enriched user experience, we have redesigned the **Hunting** tab and added the following details:

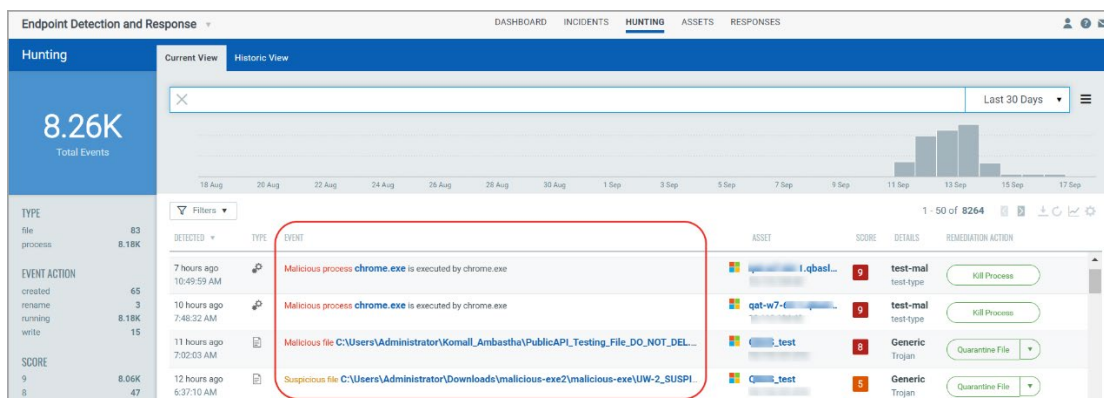
- Renamed the **Active View** to **Current View**.



- Added two sub-tabs under the Hunting tab:
  - Current View**: This tab lists all the active events on the assets.
  - Historic View**: This tab lists all the events registered and executed on the asset.



- Renamed the **Object** column to **Event**.
- To give you detailed information about the registered event, we have now modified the information displayed under the **Event** column.




## View Events Detail Page

For better clarity and understanding about the events registered on the **Hunting** tab, we have revamped the **Events Details** page and added the following information:

- We have added a new **Parent Process** section. This section gives you complete information about the parent process of the registered event.

Parent Process	
State	RUNNING
Name	<a href="#">setup.exe</a>
Full Path	<a href="#">C:\Windows\Temp\CR_58B7D.tmp\setup.exe</a>
Arguments	"C:\Windows\TEMP\CR_58B7D.tmp\setup.exe" --install-archive="C:\Windows\TEMP\CR_58B7D.tmp\CHROME.PACKED.7Z"
Elevated	false
Username	NT AUTHORITY\SYSTEM
ID	2038
Event ID	RTP_0b83a56d-879b-4ade-9446-c0289f43d05e_-459611612325009

- We have added the following details about the asset on which the event is registered.

Asset Details	
	<b>WINR2-QB</b> OS:WINDOWS
IPv4	10.115.1.210
IPv6	—
Last User Login	Administrator
Last Activity	Aug 27, 2020 12:36 PM



## New Tokens

We have added the following new tokens on the Hunting tab:

- **parent.name:** This token allows you to find events created by a process.
- **parent.pid:** This token allows you to find events for a parent process ID.
- **parent.imagepath:** This token allows you to find events with the parent process image path.
- **parent.event.id:** This token allows you to find events with the parent process event id.

For more information on the token usage, see the **Hunting** tab on the EDR UI.