



Qualys Endpoint Detection and Response v3.x

Release Notes

Version 3.0

November 30, 2023

Here's what's new in Qualys Endpoint Detection and Response 3.0!

What's New

[Updated OnAccess Scan in Anti-malware Profile](#)

[Updated Forensic Script and the Default Download Folder](#)

[Introduced New Tokens](#)

[Introduced New Dashboard: Endpoint Detection Response Overview](#)

[Included Monthly Recurrence to OnDemand Scan Settings](#)

Qualys Endpoint Detection and Response 3.0 brings you some improvements and updates!

Updated OnAccess Scan in Anti-malware Profile

The OnAccess Scan feature is enhanced with scan setting type options such as **Aggressive**, **Normal**, **Permissive**, and **Custom**. This new scan setting type provides security against malware and improves the network performance.

The following screenshot is an example of Normal Scan Setting:

Create New : Anti-malware Profile

STEPS 2/10

- General Settings
- OnAccess Scan**
- OnDemand Scan
- Behavioral Scan
- Network Protection
- Network Attack Defense
- Assets
- Device Control
- Exclusions
- Review and Confirm

OnAccess Scan

Enable OnAccess Scan to monitor system activity and block malware. ☒

Scan Setting

Select the Scan Setting type to provide security against malware and enhance the network performance.

☐ Aggressive ☒ Normal ☐ Permissive ☐ Custom

Normal Setting scans all accessed files from local drives and application files from network drives. It does not scan archived and zero-risk files.

Normal Scan Setting

File Actions for Malicious Detection		
Scan Local File Type All Files	Scan Network File Type All Files	Maximum size (MB) Disabled

Scan Details for Malicious Detection		
New or Changed Files Enabled	Boot Sectors Enabled	Process Memory Disabled
keyloggers Enabled	Archive Scanning Disabled	Archive Maximum Depth Disabled
Archive Maximum Size (MB) Disabled	PUA Scan Enabled	Deferred Scanning Enabled

Actions for Infected and Suspected Files		
Infected File - Primary Action Move to Quarantine	Infected File - Secondary Action Deny	Suspected File - Primary Action Move to Quarantine
Suspected File - Secondary Action Deny		

Quarantined Files Restore Location
C:/Documents/Quarantine_Files

Fileless Attack Protection

Select the Command-Line Scanner option to automatically allow Qualys to discover and block file attacks at the pre-execution stage.

☒ Command-Line Scanner

Optional OnAccess Scan Settings

Select any of the following optional OnAccess Scan Settings options.

☒ Retain a Backup File Copy
Select this option to disinfect the original file and save and quarantine a copy of the file.

☒ Linux Directories Scan Settings
Select this option to scan Linux Directories. Add the directories from the Directories drop-down.

Directories

Select Directories

Remove Selected ☐ DIRECTORIES 0 - 1 of 1

DIRECTORIES	ACTIONS
/etc	<input type="checkbox"/> <input type="button" value="X"/>

For more information, see OnAccess Scan in [EDR Online Help](#).

Updated Forensic Script and the Default Download Folder

To gather window logs and registry services, the Forensic script is updated with the following:

- **Event Log**- Windows Defender, Windows Powershell, and Windows Sysmon
- **Persistence**- hklm\System\Controlset\00x_Services_Bam

Note: From this release, the data downloaded for all successful data requests is in a .7z folder of your local system.

For more information, see Scripts Executed on Forensics in [EDR Online Help](#).

Introduced New Tokens


- **asset.architecture**- Use the **asset.architecture** token to filter Mac assets based on its architecture. The token uses the input value as string.
- **incident.platform**- This token filters incidents based on the asset platform. The **incident.platform** token requires the input value as string.
- **parent.iscertificateexists**- Use **parent.iscertificateexists** token to view the list of events with certificates available for the parent. Use the boolean value true or false to view the list.
- **parent.iscertificatevalid**- This token lists all the events that have a valid certificate for a parent.
- **event.isdetectedbyepp**- To view the list of the events detected by EPP, use this token. The token requires the input value in a boolean value, true or false.
- **event.threatname**- For **event.threatname** token, use the input value as text to find events with the specific threat name.
- **event.detectiontype**- Use the **event.detectiontype** token to list all the events with a particular detection type. The token requires the input value as string.
- **parent.productname**- Use the boolean value true or false as the input parameter for the **parent.productname** token to list all the events whose parent matches the given product name.
- **process.productname**- This token lists all the process events with a particular product name. The **process.productname** token requires the input value as string.
- **process.sid**- This token lists all the process events with a particular security identifier (sid). The string parameter is the input value required for this token.
- **process.iscertificateexists**- This token lists all the process events that have certificates available. The token **process.iscertificateexists** requires the boolean value as true or false.

For more information, see Search Tokens in [EDR Online Help](#).

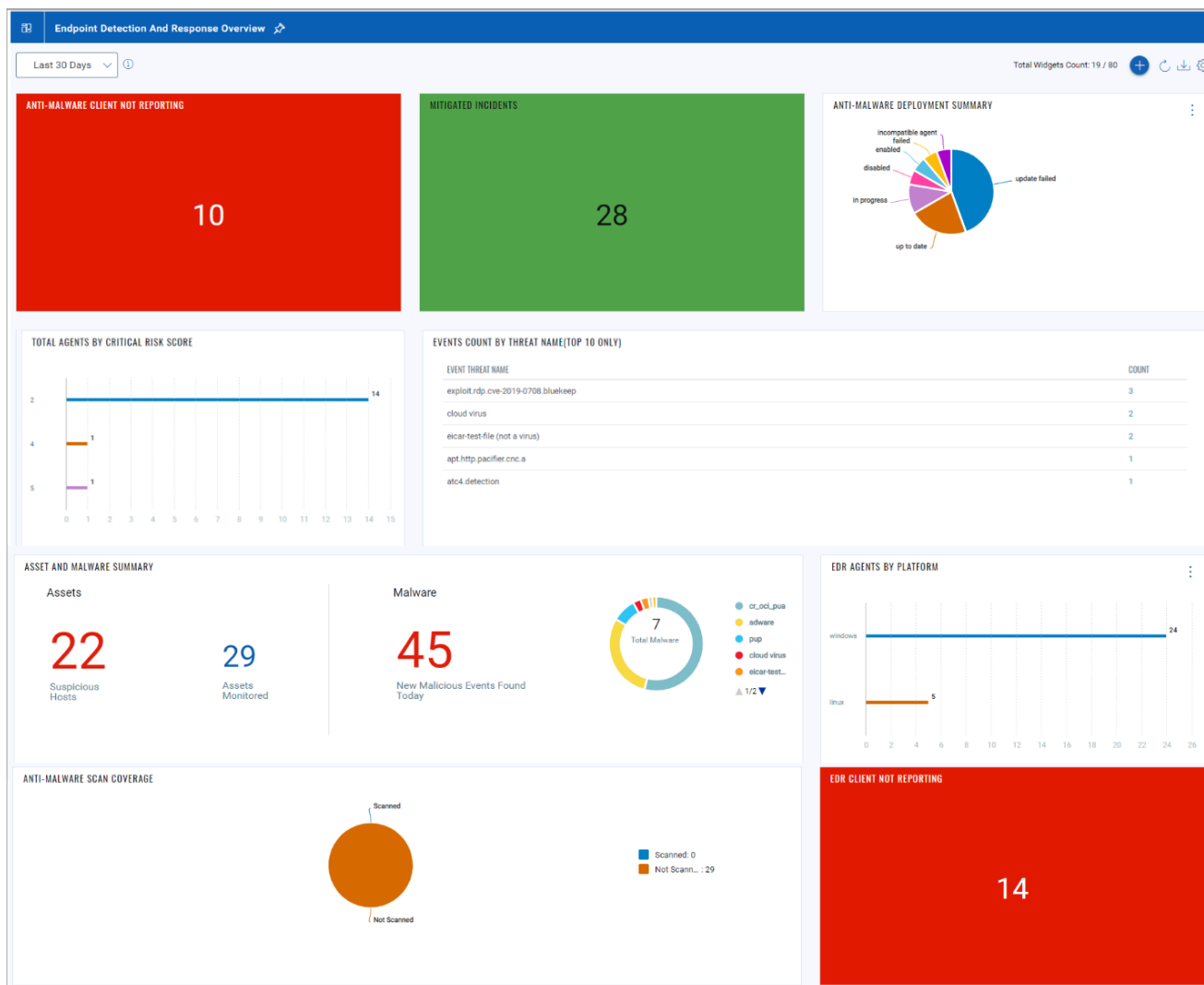
Introduced New Dashboard: Endpoint Detection Response Overview

Our new **Endpoint Detection Response Overview** dashboard enhances your dashboard experience by providing a central location to visualize your assets, anti-malware coverage, mitigated incidents, device control activity, and more. The essential findings are highlighted in a summarized manner.

Perform the following steps to view the **Endpoint Detection Response Overview** dashboard:

1. Navigate to **Dashboard**.
2. Click the Dashboard Picker  icon and select **Endpoint Detection Response Overview** dashboard.

The following screenshot of the Dashboard lists the various widgets and the details in each widget:



Refer to the following table to know about the widget description:

Widget	Description
Anti Malware client not reporting	Shows the count of assets where anti-malware is enabled, and assets have not been reported from the last 1 day.
Mitigated incidents	Shows the count of mitigated incidents for all the anti-malware.
Antimalware deployment summary	Shows the count of assets with the status of the deployed anti-malware.
Count of quarantined assets	Shows count of quarantined assets
Anti-malware profile coverage	Shows the count of anti-malware enabled assets with active state and the name of the antimalware profile associated with them.
Anti-malware coverage	Shows a count of currently active assets with anti-malware either enabled or disabled.
Total agents by critical risk score	Shows the count of active anti-malware enabled assets with their criticality score.
Events count by threat name	Shows the number of events categorized based on the associated threat name.
Events count by threat type	Shows the number of events categorized based on the type of threat to which they belong.
Device control activity	Shows the count of events categorized by action taken on them, such as Allowed, Blocked, and Read-only.
Asset scan status	Shows the count of assets that are categorized based on antimalware scan status.
Anti-malware scan coverage	Shows the count of assets scanned or not scanned for anti-malware from the last 7 days.
EDR client not reporting	Shows count of anti-malware enabled assets that are not reported from the last 1 day.
Asset and malware summary	Shows the count for suspicious hosts, assets monitored, the total number of malware, and new malicious events found today.
EDR agents by platform	Shows the count of active assets and their platforms.
Malicious event summary	Shows event summary on files, processes, networks, and the total number of malicious events in the last 7 days.
Incident status	Shows the count of incident status as open, closed, or in progress.
Multiple re-occurrence of unique infections	Shows count of re-occurrences of unique infections such as cloud viruses and adware on specific assets.
Asset count by malware-family	Shows the number of assets categorized by their respective malware families.

Included Monthly Recurrence to OnDemand Scan Settings

With this release, you can perform monthly **OnDemand Scan** in addition to the previously available daily and weekly options. You can edit the existing anti-malware profile for monthly scans or create a new profile. To schedule a monthly OnDemand Scan, perform the following steps in the **Anti-malware Profile** under the **Configuration** tab:

1. Click **New Anti-malware Profile** or edit an existing profile.
2. Go to **OnDemand Scan**.
3. In the **Others** section, select **Recurring Scan**. From the **Recurrence** drop-down, select **Monthly**. In the **Occurs every (in months)**, select the recurrence period. For example, if you want to perform an OnDemand monthly scan thrice a month, select 3 in the Occurs every drop-down.

The following screenshot is an example of a Monthly OnDemand Scan with a recurrence period of three:

The screenshot shows the 'Anti-malware Profile Details' configuration page. On the left, a sidebar lists steps 1 through 10, with 'OnDemand Scan' (step 3) highlighted with a red box. The main content area is titled 'OnDemand Scan' and has a toggle switch turned on. Below the title, there is a description: 'Add and configure system scans for malware that will run regularly on the target computers, according to the defined schedule.' A note states: 'Enable this option to treat the potentially unwanted application (PUA) file as a normal malware and take action. If not enabled, only the PUA detection is reported.' Under the 'Others' section (highlighted with a red box), the 'Retain a Backup File Copy' checkbox is checked. Below this, there are fields for 'Start Date' (10/06/2023) and 'Start Time' (02:18 PM). The 'Recurring Scan' checkbox is also checked and highlighted with a red box. Below it, the 'Recurrence' dropdown is set to 'Monthly' and the 'Occurs every (in months)' dropdown is set to '3'. At the bottom, there are 'Cancel', 'Previous', and 'Next' buttons.

For more information, refer to the OnDemand scan section [EDR Online help](#).