



# Qualys Endpoint Detection and Response v1.x

## Release Notes

Version 1.5

May 13, 2021

Here's what's new in Endpoint Detection and Response 1.5!

[Enhanced Incidents Tab](#)

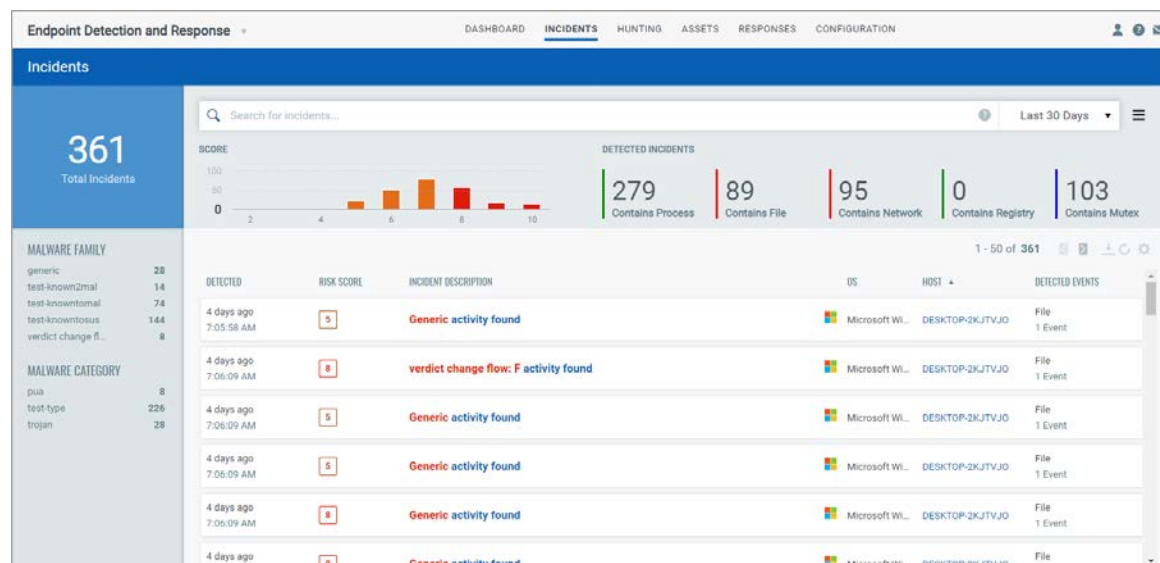
[Active Threats By Host tab moved to Assets Tab](#)

[Support for Non-Portable Executable Files](#)

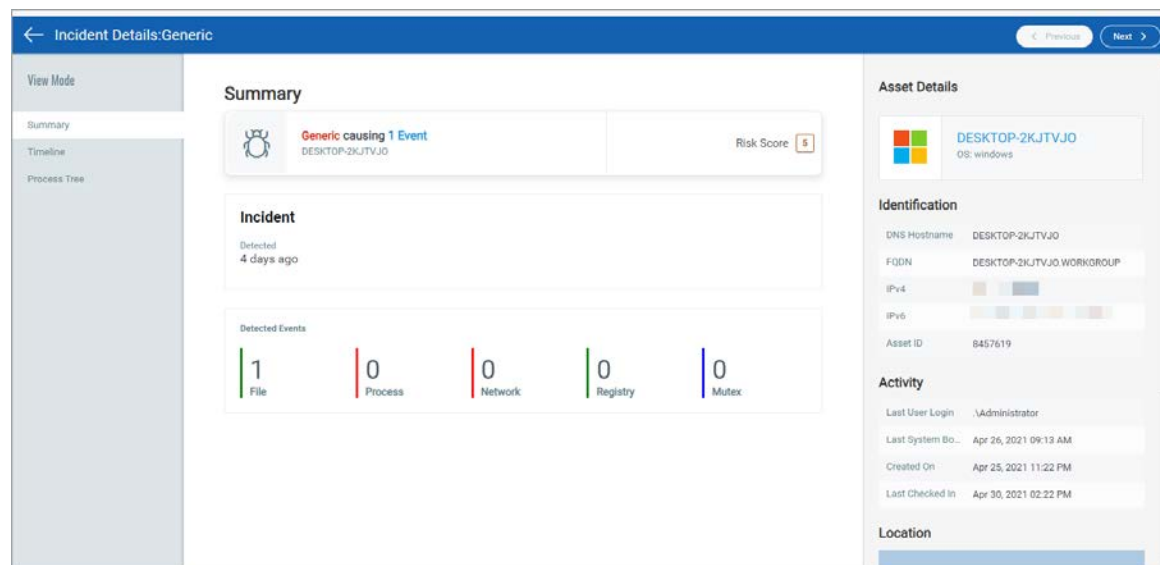
Endpoint Detection and Response 1.5 brings you more improvements and updates! [Know more](#)

## Enhanced Incidents Tab

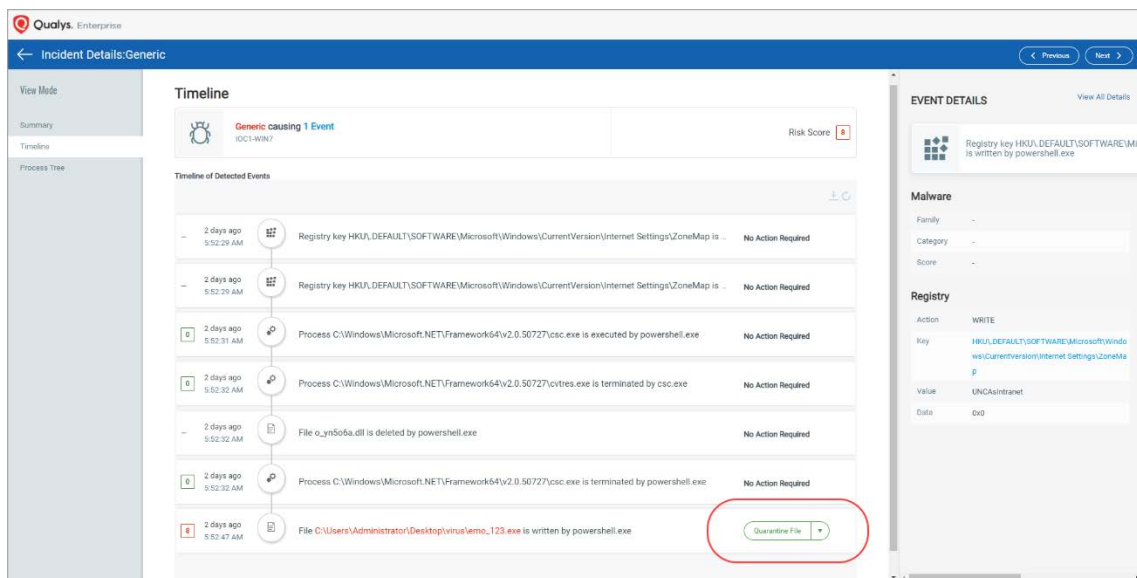
We have enhanced the Incidents tab so as to show all the incidents detected on an asset. You can view the OS and host on which the incident was detected, the events detected, and other information at a quick glance.



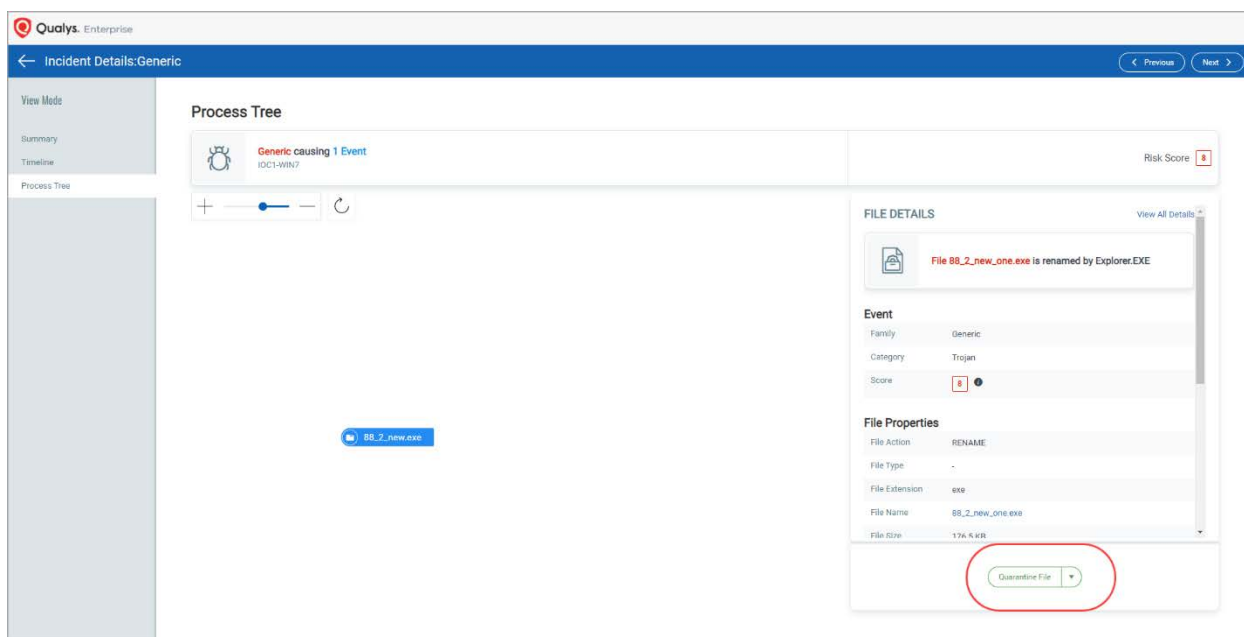
To know more about the incident, click on the incident description and in the Incidents Details, view information like Timeline, Process Tree, Asset Details, etc. If the risk score is zero, then the incident is considered remediated or non malicious.



Incidents can also be remediated from the Incident Details. Navigate to the Timeline tab to view the timeline of the detected event and choose a remediation action if applicable.



You can also take remediation action from the Process tree tab.



We have added the following new QQL tokens for you to search incident details on the Incidents tab:

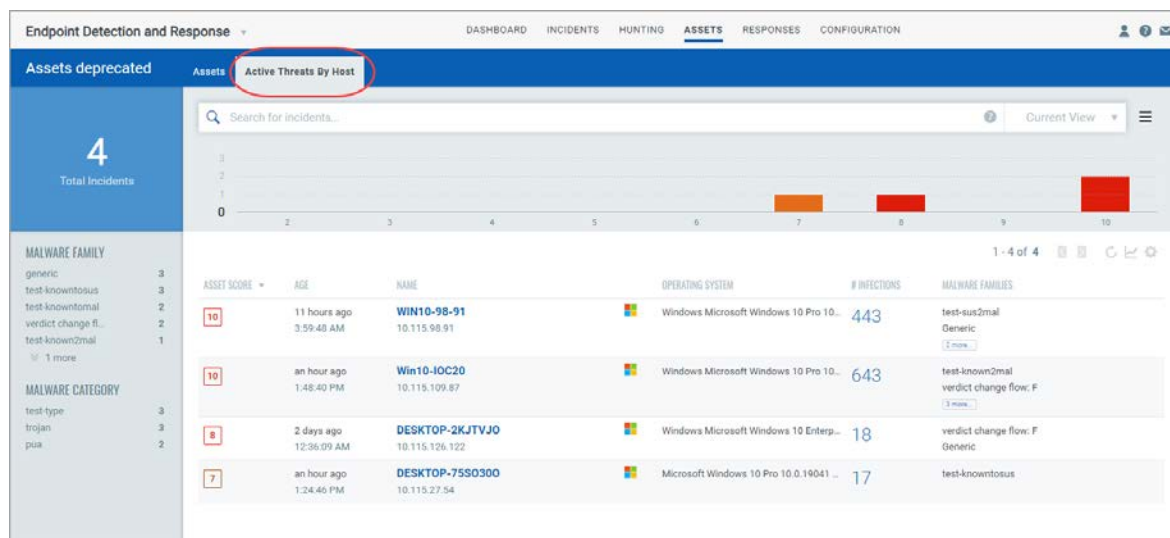
- **incident.malware.family**: This token will help you find incidents that belongs to a malware family
- **incident.malware.category**: This token will help you find incidents that belong to a certain malware category
- **incident.id**: This token will help you find incidents by its unique id
- **incident.asset.agentid**: This token will help you find incidents by agent id
- **incident.files**: This token will help you find incidents by number of file events present in the events time line
- **incident.registry**: This token will help you find incidents by number of registry events present in the events time line

- **incident.process:** This token will help you find incidents by number of process events present in the events time line
- **incident.mutex:** This token will help you find incidents by number of mutex events present in the events time line
- **incident.network:** This token will help you find incidents by number of network events present in the events time line
- **incident.riskscore:** This token will help you find incidents by their risk score
- **incident.detectedon:** This token will help you find incidents by date and time on which the incident was detected
- **incident.eventtype:** This token will help you find incidents by the type of the events present in the events time line. You can choose from: FILE, NETWORK, PROCESS, REGISTRY, MUTEX
- **incident.asset.hostname:** This token will help you find incidents by their hostname
- **asset.operatingsystem:** This token will help you find incidents by their agent id

## Active Threats By Host tab moved to Assets Tab

We have relocated the Active Threats By Host tab from the Hunting tab to the Assets tab for better usability.

Here you view assets that have active threats and details like asset score, the number of infections, malware family the threat belongs to, etc.



## Support for Non-Portable Executable Files

With this release, we have added support for Non-Portable Executable Files. All the detected non-Portable Executable (non-PE) files are listed in the Current View of the Hunting tab. Navigate to a non-pe file, and in the event details section, you can view the details of the file as well as Parent Process and Process Tree details.

For example, if it is a .pptx file, you can view the following details in your event details Summary:

The screenshot shows the 'Event Details' page for the file 'Introduction to cloud.pptx'. The page is divided into three main sections: a left sidebar, a central 'Summary' section, and a right 'Asset Details' section.

**Left Sidebar:** Contains 'VIEW MODE' and a list of tabs: 'Summary', 'Parent Process', and 'Process Tree'. 'Summary' is currently selected.

**Summary Section:** Displays file details in a table format. A red box highlights the following information:

File		
File Action	File Type	File Extension
WRITE	-	pptx
Macro Enabled	File Name	File Size
No	Introduction to cloud.pptx	971.11 KB
Created On	Modified On	Accessed On
Apr 12, 2021 11:34 PM	Apr 13, 2021 12:04 AM	Apr 13, 2021 12:14 AM
Author	Last Modified By	Creating Application
[User Icon]	[User Icon]	Microsoft Office PowerPoint
Title	Pages	Version
Introduction to cloud	7	-
Path	Full Path	MD5
C:\Users\Administrator\...	C:\Users\Administrator\...Introduction to cloud.pptx	9ce94e238571e74245e74d...b317601e0
SHA256 d1750735d827668572653d31c0761a0fcc5a3c4404dea7b054e3e23370c5		

**Asset Details Section:** Displays information about the asset 'WIN10-98-91'.

**Identification:**

DNS Hostname	WIN10-98-91
FQDN	WIN10-98-91.WORKGROUP
IPv4	10.115.98.91
IPv6	-
Asset ID	8179389

**Activity:**

Last User Login	.Administrator
Last System Bo...	Apr 29, 2021 11:27 PM
Created On	Mar 24, 2021 02:56 AM
Last Checked In	Apr 30, 2021 03:12 PM

**Location:**

We have added the following new QQL tokens for you to search non-pe file details on the Hunting tab:

- **file.title:** This token will help you find events of the specified file title.
- **file.author:** This token will help you find events of the specified file author
- **file.lastmodifiedby:** This token will help you find files that were last modified by the specified author
- **file.creatingapplication:** This token will help you find files that are created by using the specified application
- **file.numofpages:** This token will help you find files by the number of pages present in the file
- **file.ismacroembedded:** This token will help you find files that have Macro code embedded in the file
- **file.nonpefile:** This token will help you find files that are of non PE file type
- **file.pdf.pages:** This token will help you find files by the number of pages present in the PDF file
- **file.pdf.js:** This token will help you find files by the value of /JS field in the PDF file header
- **file.pdf.javascript:** This token will help you find files by the value of /JavaScript field in the PDF file header
- **file.pdf.embeddedfile:** This token will help you find files by the value of /EmbeddedFile field in the PDF file header
- **file.pdf.objstm:** This token will help you find files by the value of /ObjStm field in the PDF file header
- **file.pdf.aa:** This token will help you find files by the value of /AA field in the PDF file header
- **file.pdf.openaction:** This token will help you find files by the value of /OpenAction field in the PDF file header

## Issues Addressed

- We have fixed the issue, and the pagination order is now maintained correctly after the user navigates back to the Hunting tab after viewing the incident details.
- The issue is now resolved, and the Process Tress tab is loaded accurately for the event details.
- The issue of internal error being displayed is now fixed, and the remediation actions are now completed appropriately.
- The EDR tab of the Asset Details is now loaded correctly even after the user switches between other tabs.