Qualys Endpoint Detection and Response v2.x

Release Notes

Version 2.7

October 17, 2023

Here’s what’s new in Qualys Endpoint Detection and Response 2.7!

What’s New

Qualys Endpoint Detection and Response 2.7 brings you some improvements and updates!

Endpoint Protection Platform for MacOS

Endpoint Protection Platform (EPP) onboarding for MacOS is now supported. The EPP onboarding is supported for MacOS 12.x and 13.x versions. From this release, EPP supports the following features:

- On-access scanning for real-time antimalware protection.
- Block known phishing web pages.
- Scan web traffic in real-time to prevent malware from being downloaded.

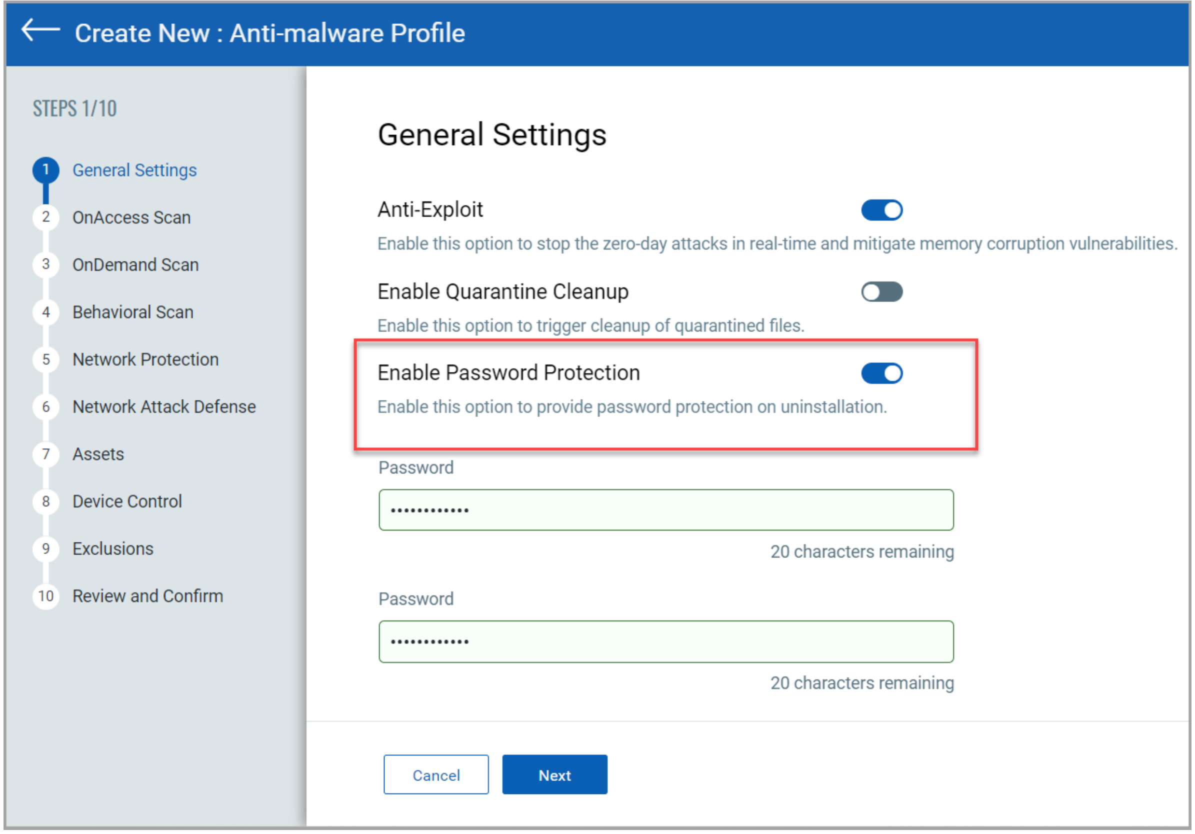
For more information, see EPP Onboarding for MacOS in *EDR Online Help*.

Enhanced Anti-malware Profile Details Page

The **Anti-malware Profile Details** page now includes the **Enable Password Protection** option in the **General Settings,** sections.

- **Enable Password Protection in General Settings**- This setting avoids removing anti-malware applications without authorization.

  The following screenshot is an example of the **Enable Password Protection** option enabled in the **Anti-malware Profile** settings.



General Settings

Anti-Exploit ●
Enable this option to stop the zero-day attacks in real-time and mitigate memory corruption vulnerabilities.

Enable Quarantine Cleanup ○
Enable this option to trigger cleanup of quarantined files.

Enable Password Protection ●
Enable this option to provide password protection on uninstallation.

Password
••••••••••••
20 characters remaining

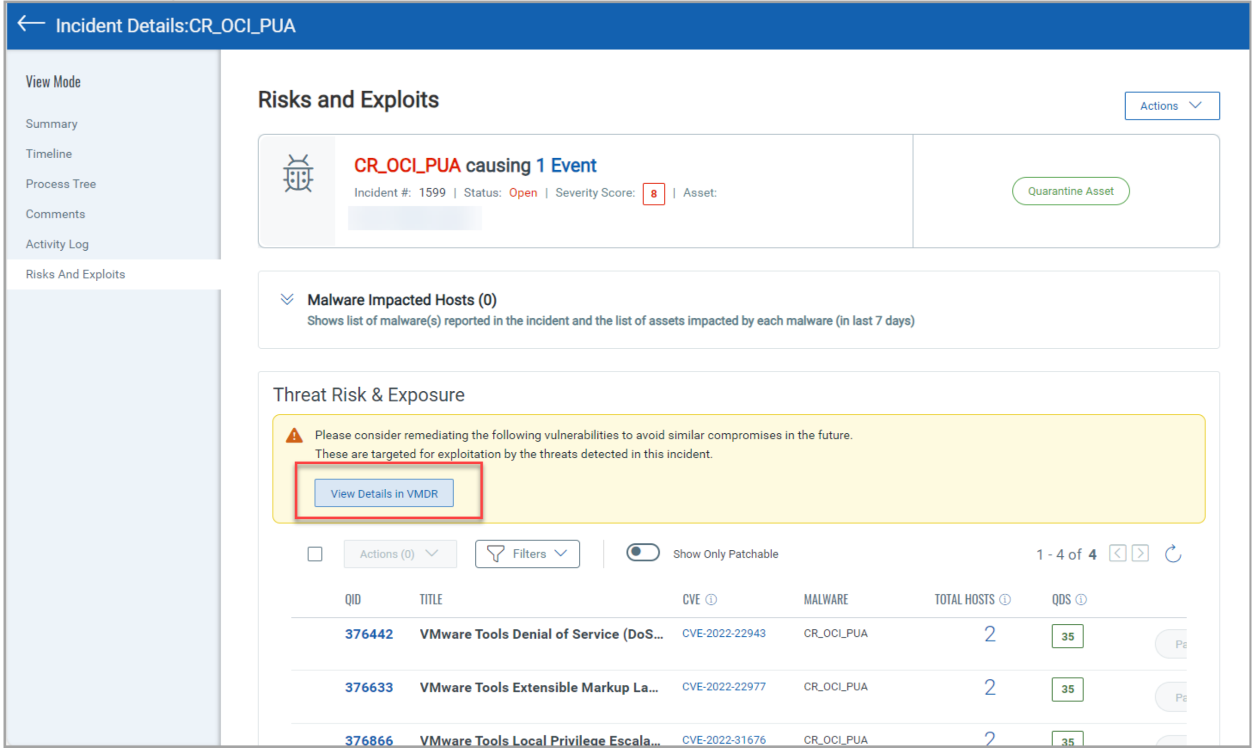
Password
••••••••••••
20 characters remaining

For more information, see General Settings in *EDR Online Help*.

Detect and Patch Incidents in Incident Details

Along with detecting incidents in the VMDR, you can now patch the incidents. We have now integrated VMDR and Patch Management applications in EDR. From the **Incidents** tab, hover the mouse on any of the assets to view the **Quick Actions** menu and click **Incident Details**. In the **Risks and Exploits** section, click **View Details in VMDR** to view the vulnerabilities and **Patch Now** to patch the vulnerabilities.

The following screenshot is an example of **View Details in VMDR**:



Risks and Exploits

CR_OCI_PUA causing 1 Event

Incident #: 1599 | Status: Open | Severity Score: 8 | Asset:

[redacted]

Malware Impacted Hosts (0)

Shows list of malware(s) reported in the incident and the list of assets impacted by each malware (in last 7 days)

Threat Risk & Exposure

Please consider remediating the following vulnerabilities to avoid similar compromises in the future.
These are targeted for exploitation by the threats detected in this incident.

QID	TITLE	CVE	MALWARE	TOTAL HOSTS	QDS	
376442	VMware Tools Denial of Service (DoS...	CVE-2022-22943	CR_OCI_PUA	2	35	Pa
376633	VMware Tools Extensible Markup La...	CVE-2022-22977	CR_OCI_PUA	2	35	Pa
376866	VMware Tools Local Privilege Escala...	CVE-2022-31676	CR_OCI_PUA	2	35	

For more information, see Incident Details in *EDR Online Help*.

Updated Forensics Scripts

We have updated the forensics script with the following:

- Security Event Log
- Persistence data
- SMB outbound sessions
- Prefetch files

For more information, see Scrips Executed on Forensics in *EDR Online Help*.