Qualys Cloud Agent Windows 4.4

We are excited to tell you about new features, improvements, platform coverage changes, and fixes in this Cloud Agent release. These updates are specific to the agent binary. Platform updates for new features and fixes of management, syncing, tagging, and reporting capabilities of Cloud Agents are documented in the Cloud Platform and Cloud Suite release notes.

New Features

- Added Support for following features in File Integrity Monitoring
  - Support for file content change tracking (pending File Integrity Monitoring (FIM) backend support)
  - Support for 'File Reputation and Trust feature' (pending File Integrity Monitoring (FIM) 3.0)
- Added support for following features in Endpoint Detection and Remediation (EDR 1.5 required)
  - Added support for non-PE file events.
  - Live network event detections using Kernel component - Network Event Detection and Reporting.
  - Added support for collecting file event based on extension present in EDR policy.
  - Exclusion based on Actor process information.

Enhancements

- Support for Delay and Randomize of VM/PC scanning (pending platform support)
- Additional protections of the Agent binary

Behavior Changes

There is an additional parameter required for new installations of the Windows Agent: "webserviceuri". This parameter is provided in the installation instructions provided in the Qualys UI. This parameter is not required for pre-4.4 versions of the Agent and only required for new Agent installations.

Network driver (qnetmon) using Windows Filtering Platform (WFP) for EDR.

Fixed Defects

The following reported and notable issues have been fixed in this release.

CRM-74149	Fixed an issue where the Agent was using higher than expected CPU in certain scenarios
CRM-67733	Cloud Agent Uninstall Leaves Remnants of Previous Instance
CRM-63343	Fixed an issue where Patch Management reboot messages were not behaving as expected

The following reported and notable issues have been fixed in 4.4.1.5 hotfix release.

CRM-77288	Improved file permission handling for FIM and EDR
CRM-79561	Fixed an issue where driver did not get upgraded
CRM-80219	Fixed an issue where threads go into a suspend state
NA	Binary download improvement for auto upgrade

The following reported and notable issue has been fixed in 4.4.1.7 hotfix release.

CRM-80380	Fixed an issue where high memory was seen with FIM or EDR modules enabled while many processes were getting created and terminated Refer to the Support Article for additional information

Known Limitations and Workarounds

1. Windows 7, Windows Server 2008 R2 supports EDR and FIM only with SHA2 update.
   KB article numbers: 4474419
   More information: https://support.microsoft.com/help/4474419