

CylancePROTECT® Feature Focus

Linux Agent

CYLANCE™



Executive Summary

The CylancePROTECT 1430 agent release introduces enhanced functionality optimized for several popular operating systems and other customer-driven advancements including:

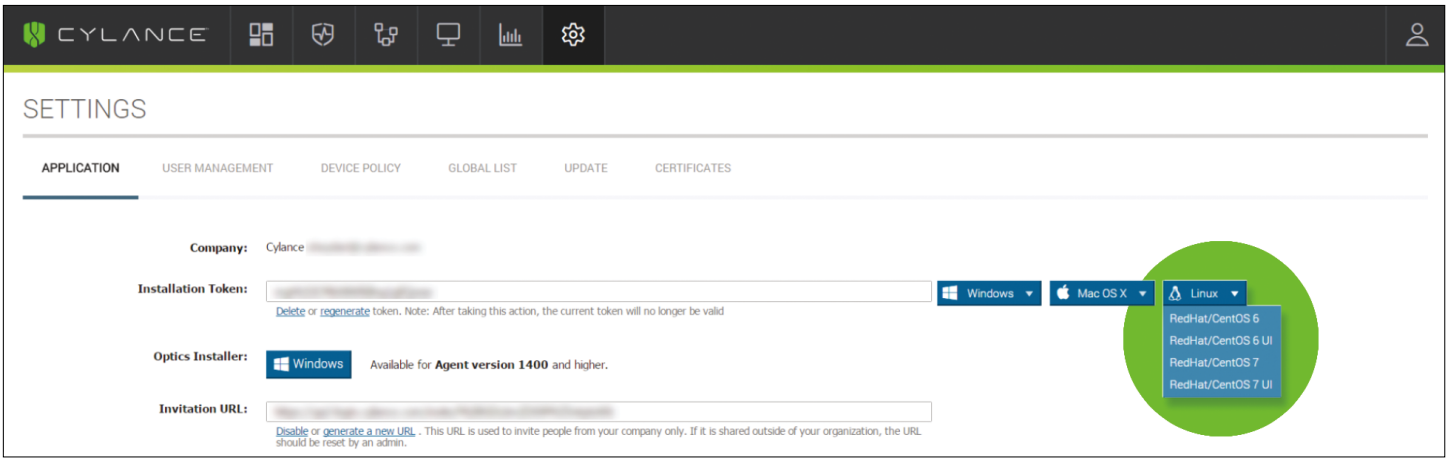
- A Linux agent
- A manual agent policy update for MacOS and Linux
- Decoupled script control management
- A quarantine hash from command line
- Improvements to increase functionality, usability and the inherent protection value to customers and prospects

New Features Matrix

Feature	Description	Customer Benefit
Linux Agent	An agent installer and application has been built to support Linux Red Hat / CentOS versions 6 and 7.	Organizations with Linux devices can now enjoy CylancePROTECT security and manage their Linux, macOS, and Windows devices from the cloud-based centralized management console.
Manual Agent Policy Update (macOS and Linux)	New feature for macOS and Linux devices which enables agent to manually check for a new policy and for verification that a policy update occurred.	Enhanced policy troubleshooting, manual policy lookup trigger, and validation of when a policy was last updated.
Quarantine File Time Threshold	Set a specified number of days in management console to keep quarantined files before automatically deleting them from agent.	Enables admins to keep their quarantine folder clean on agent devices.
Decoupled Script Control Management	Ability to manage the enablement of script control for specific script types.	The admin can now independently enable script control for Active Script, PowerShell, and Office Macros script types.
Quarantine Hash from Command Line	Admins can utilize the Windows command line to quarantine a specific file hash on a device.	Provides the ability to add files to the quarantine on devices which are offline and do not have access to the management console.

New Features Detail

Linux Agent



CylancePROTECT is now available for Linux Red Hat / CentOS versions 6 and 7. With memory protection on Linux, the agent prevents exploitation by watching behaviors on the device that indicate a compromise. Application control can be used to lock down systems so that no additional changes can be made. This is beneficial for securing Linux server environments that do not experience a high rate of change. The Linux agent supports the following operating systems:

- Red Hat Enterprise Linux / CentOS 6.6 - 32-bit and 64-bit
- Red Hat Enterprise Linux / CentOS 6.7 - 32-bit and 64-bit
- Red Hat Enterprise Linux / CentOS 6.8 - 32-bit and 64-bit
- Red Hat Enterprise Linux / CentOS 7.0 - 64-bit
- Red Hat Enterprise Linux / CentOS 7.1 - 64-bit
- Red Hat Enterprise Linux / CentOS 7.2 - 64-bit
- Red Hat Enterprise Linux / CentOS 7.3 - 64-bit

Organizations can now utilize CylancePROTECT to protect their entire device ecosystem consisting of Windows, macOS, and Linux devices.

Manual Agent Policy Update for macOS and Linux

The agent UI now displays the date and timestamp of the last policy update. This supports the ability to verify from the agent UI that a policy change has been communicated to the device. The policy timestamp can be found in the About screen after right-clicking the CylancePROTECT icon from the macOS menu bar and Linux system tray.

Included with this feature is a manual check for policy updates. From the device, right-click the CylancePROTECT icon in the macOS menu bar or Linux system tray and click **Check for Policy Update**. The agent will communicate with the management console to determine if a policy update is available.

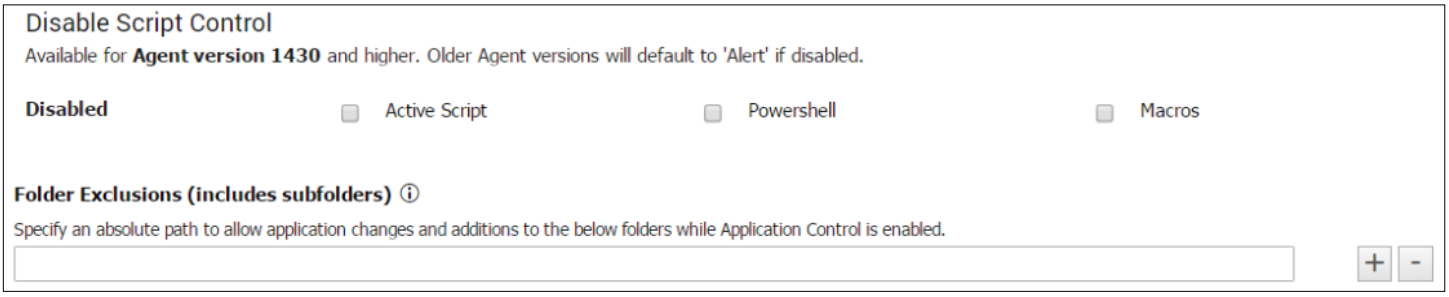
Quarantine Hash from Command Line

The Windows CylancePROTECT agent now includes the ability to quarantine a file from the command line using its hash. This is beneficial for automating the quarantine of files for groups of devices. The global quarantine is still available from the management console for quarantining files across your company's devices.

Add the command line argument '-q:<hash>' to the CylancePROTECT UI, replacing <hash> with the specific file's hash that you wish to quarantine. This will prompt the agent to send the file to quarantine. The agent currently does not provide a verification message that the file was added to quarantine.

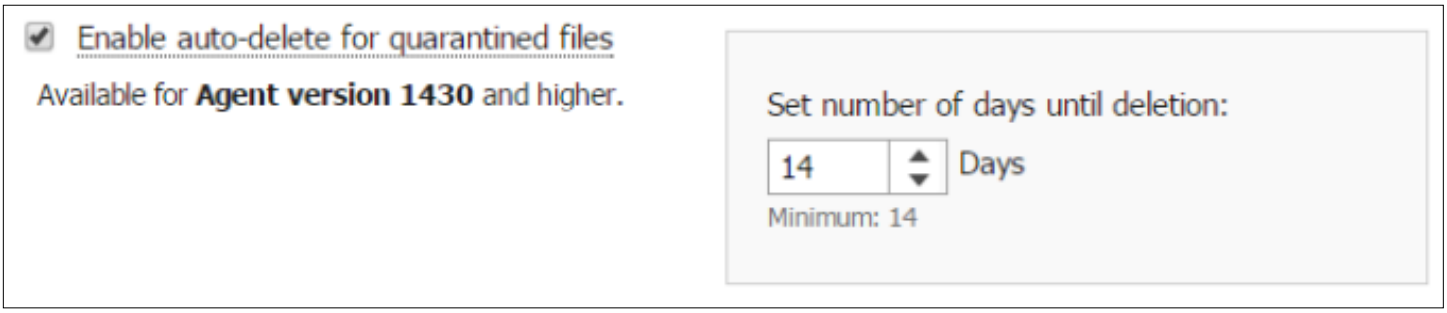
Enhancements Detail

Decoupled Script Control Management



The management console can now be utilized to independently disable script control for Active Script, Powershell, and Office Macros script types. While logged in to the management console, navigate to **Settings** → **Device Policy**, then select the policy you wish to edit and click the **Disabled** checkbox next to Active Script, Powershell, or Macros under Disable Script Control. This will disable the script control feature for the specific script types selected. The admin now has more control over the types of scripts on which they would like to use script control to alert on or automatically block scripts.

Quarantine File Time Threshold



Admins now have the ability from the management console policy to automatically delete quarantined files from an agent after X number days, where X is configurable with a minimum value of 14 days.

If enabled, the agent automatically deletes these files after the designated time. X is the number of days since the file was first quarantined. This action is included within the agent logs for verification and the file is removed from the quarantine list in the agent UI. If this feature is not enabled, the quarantined files will remain until they are manually deleted.

+1-844-CYLANCE
sales@cylance.com
www.cylance.com
18201 Von Karman Avenue, Suite 700, Irvine, CA 92612

©2017 Cylance Inc. Cylance® and CylancePROTECT® and all associated logos and designs are trademarks or registered trademarks of Cylance Inc. All other registered trademarks or trademarks are property of their respective owners.