Feature Focus: CylancePROTECT

Application Control for Fixed-Function Devices

Maintain Control of Fixed-Function Devices with Application Control

CylancePROTECT® Application Control gives organizations the ability to ensure fixed-function devices are in a pristine state continuously, eliminating the drift that may occur over time when devices are left unmanaged.

Augmenting the AI driven malware prevention capabilities of CylancePROTECT, Application Control is the easiest way to ensure fixed-function devices:

- Remain compromise free continuously
- Are available for their specific function 24x7
- Are no longer susceptible to disruptions from a successful attack

Unauthorized applications on fixed-function devices, such as an ATM or kiosk, increase the risk of a breach or compromise significantly.

To combat the risk associated with an attacker gaining access to these devices and installing a malicious app, organizations need an easy way to ensure the device is only used for its intended purpose. The Application Control capability included with CylancePROTECT provides a streamlined approach to application usage enforcement and policy management.

Harden Fixed-Function Devices

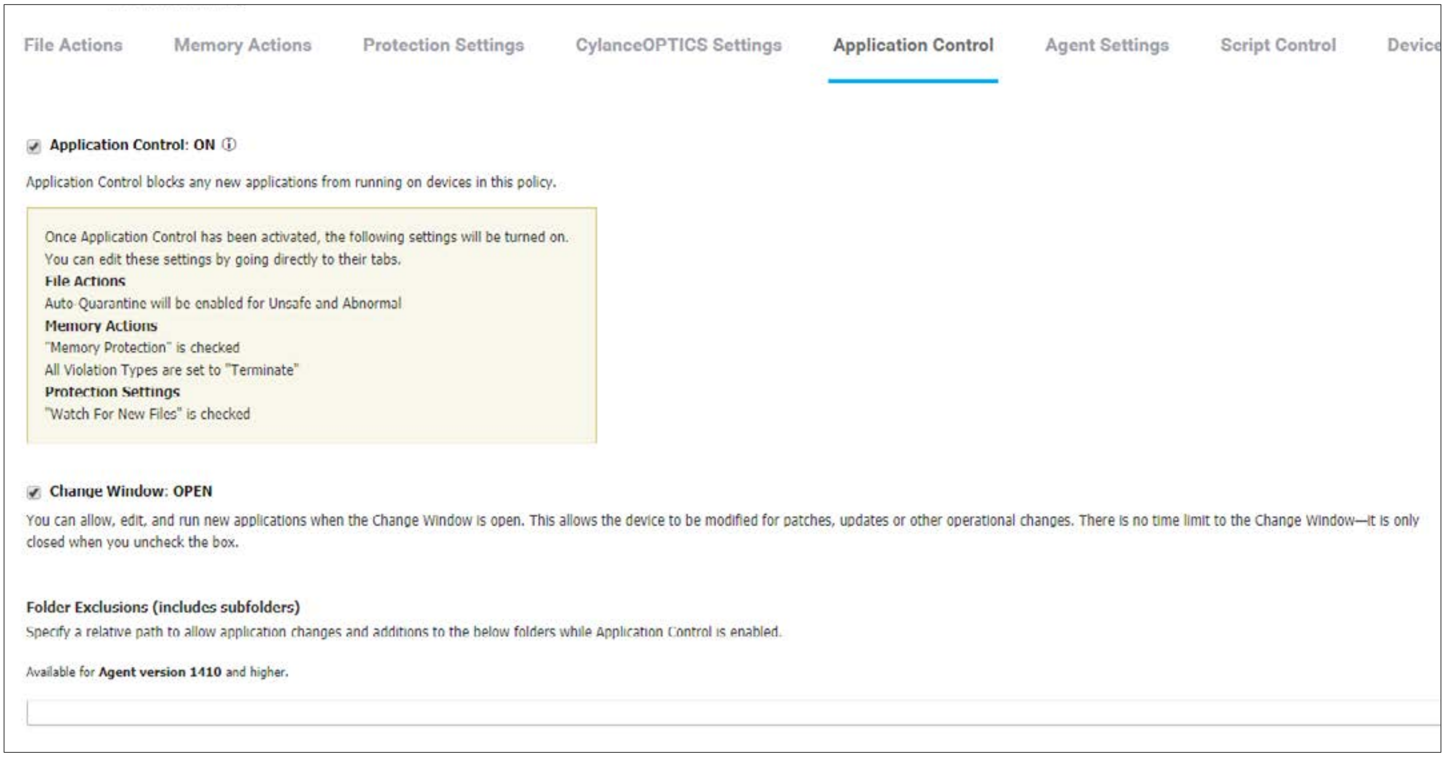
Traditionally, organizations have managed their device application stack using a blacklist that allows any application to run on the device unless the application is specifically known to be malicious or exhibits known bad behaviors. The problem, however, is that this places the responsibility on the device administrator to explicitly identify all known bad applications, which is not feasible.

CylancePROTECT Application Control takes a different approach to securing function-specific devices. Instead of forcing the administrator to become an expert in malicious applications and provide constant updates, Application Control allows the administrator to develop a “gold image” for the devices, deploy this image to the desired devices, and apply a global lockdown ensuring the device does not change. With the device in lockdown, and CylancePROTECT’s other prevention capabilities actively protecting the device, administrators can rest assured that their devices are secure.

CylancePROTECT Application Control: A Closer Look

Application Control is an optional setting that allows users to lockdown specified systems and restrict any changes on the devices after being locked down. Only the applications that exist on a device before the lockdown occurs can execute on that device. Any new applications, as well as changes to the executables of existing applications, will be denied. The Cylance® Agent Updater will also be disabled when Application Control is enabled.

When Application Control is activated, the following recommended settings will take place (see image below). With Application Control enabled, these policy settings can be edited by going directly to their tasks.



☑ **Application Control: ON**

Application Control blocks any new applications from running on devices in this policy.

Once Application Control has been activated, the following settings will be turned on.
You can edit these settings by going directly to their tabs.
File Actions
Auto Quarantine will be enabled for Unsafe and Abnormal
Memory Actions
"Memory Protection" is checked
All Violation Types are set to "Terminate"
Protection Settings
"Watch For New Files" is checked

☑ **Change Window: OPEN**

You can allow, edit, and run new applications when the Change Window is open. This allows the device to be modified for patches, updates or other operational changes. There is no time limit to the Change Window—it is only closed when you uncheck the box.

Folder Exclusions (includes subfolders)

Specify a relative path to allow application changes and additions to the below folders while Application Control is enabled.

Available for **Agent version 1410** and higher.

Change Window

The Change Window option can temporarily disable Application Control to allow, edit, and run new applications or perform updates. This includes updating the Agent.

Folder Exclusions (Including Subfolders)

An absolute path can be specified to allow application changes and additions to the specified folders while Application Control is enabled.

Key Benefits

Full Spectrem Threat Prevention

Provides a single endpoint agent that delivers continuous malware prevention, device and script control, application control, and memory exploitation protection without the use of signatures or frequent updates to the product, freeing up the analyst to address other needs from the business

Single Agent/Single Console

Enables administrators to manage all their endpoints, whether dynamic (laptops, desktops) or fixed-function (point of sale systems, ICS, ATMs) from the same web-based console, eliminating the complexity that could arise from multiple management consoles.

Full Support for Air-Gapped Networks

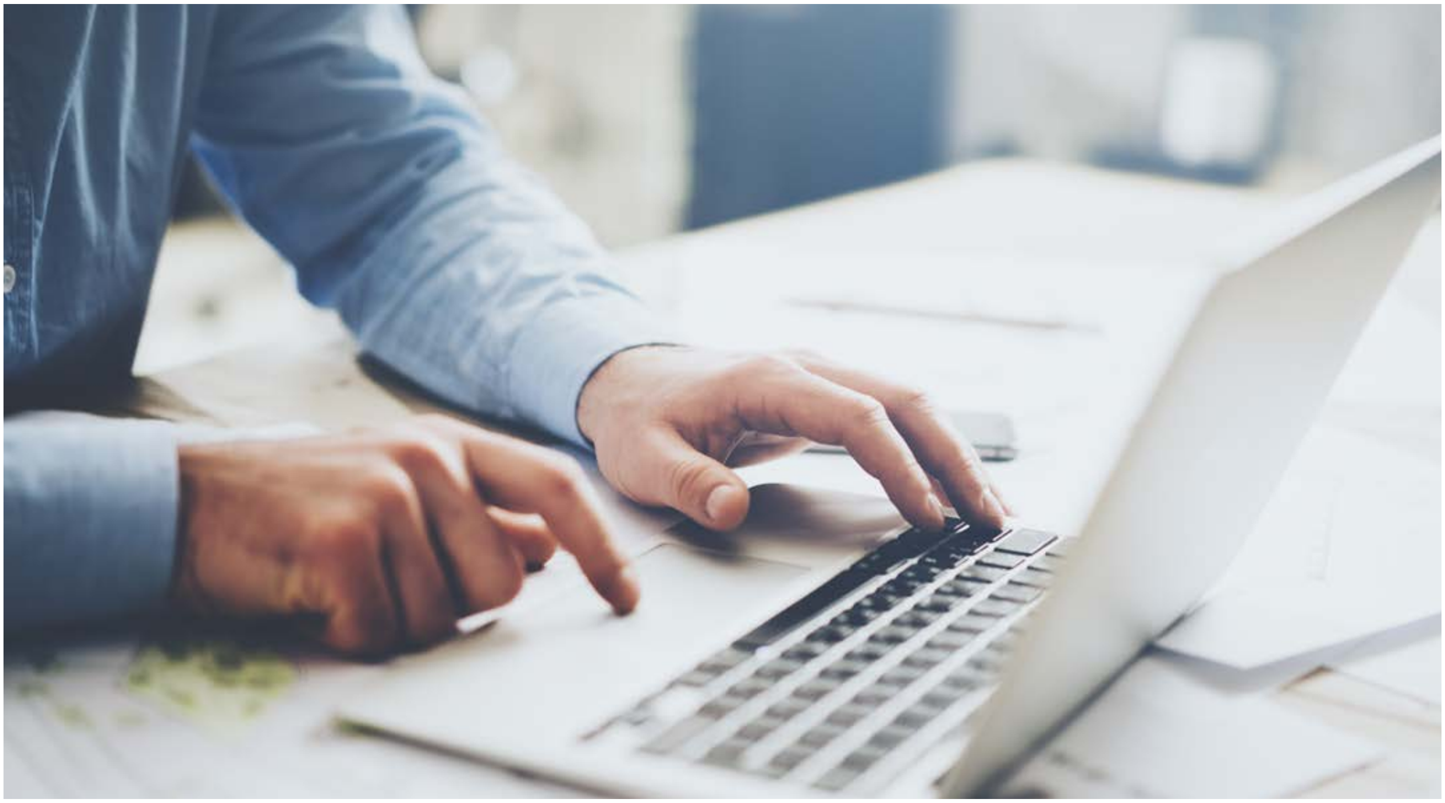
CylancePROTECT supports disconnected/air-gapped networks and is the best solution for sensitive systems like ICS, which cannot be directly connected to outside networks such as the Internet.

About Cylance

Cylance uses artificial intelligence to deliver prevention-first, predictive security products and specialized security services that change how organizations approach endpoint security.

Cylance's security solutions provide full spectrum predictive threat prevention and visibility across the enterprise, combatting threats such as malware, ransomware, fileless malware, malicious scripts, weaponized docs, and other attack vectors.

With AI based malware prevention, application and script control, memory protection, device policy enforcement, root cause analysis, threat hunting, automated threat detection and response, coupled with expert security services, Cylance can protect endpoints without increasing staff workload or costs.



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

CYLANCE