

The logo for CORVID CYBERDEFENSE is centered on a dark blue background with a network of glowing teal lines and dots. The word 'CORVID' is written in a large, bold, white sans-serif font. Below it, the word 'CYBERDEFENSE' is written in a smaller, white, spaced-out sans-serif font.

# CORVID

CYBERDEFENSE

How To Install Cylance Endpoint Security

Cylance Overview ..... 2

Windows Installation..... 3

MacOS Installation ..... 7

Minimum Requirements ..... 10

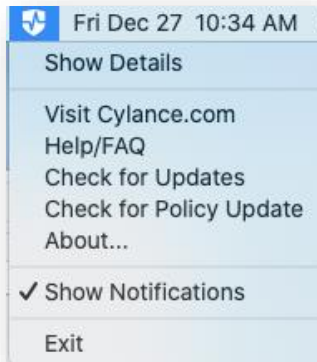
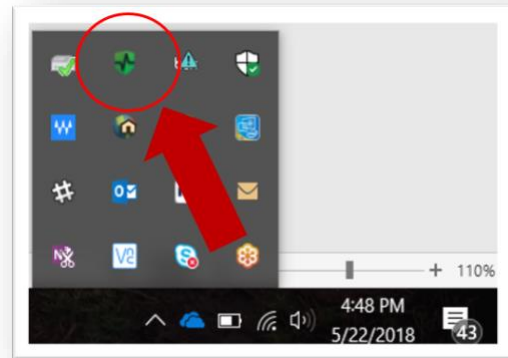
## Cylance Overview

CylancePROTECT (now called Blackberry Spark) is a next-generation anti-virus solution that utilizes machine learning to identify and block malware, such as ransomware, malicious scripts, and other advanced threats. Leveraging machine learning algorithms allows Cylance to identify threats before being seen in the wild, which are often referred to as “zero-day” threats.

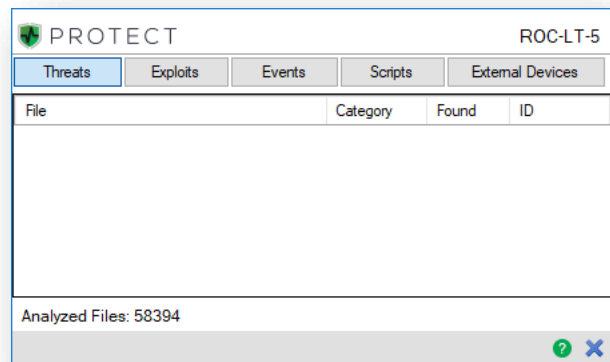
CylanceOPTICS is a detection and response add-on to CylancePROTECT that is critical for threat hunting, identifying and alerting on potentially malicious activity, and functioning as a flight recorder that captures endpoint actions leading up to a Cylance quarantined event.

Once installed, the Cylance agent will run in the background. You will see the Cylance shield icon in the Windows system tray shown right.

Or for MacOS users, the icon can be found in the notification bar, shown below.



In the event Cylance blocks a malicious file it will be listed in the Event panes inside the agent details. If a file is believed it to be blocked in error, notify Corvid Cyberdefense to investigate the file and take the appropriate action.

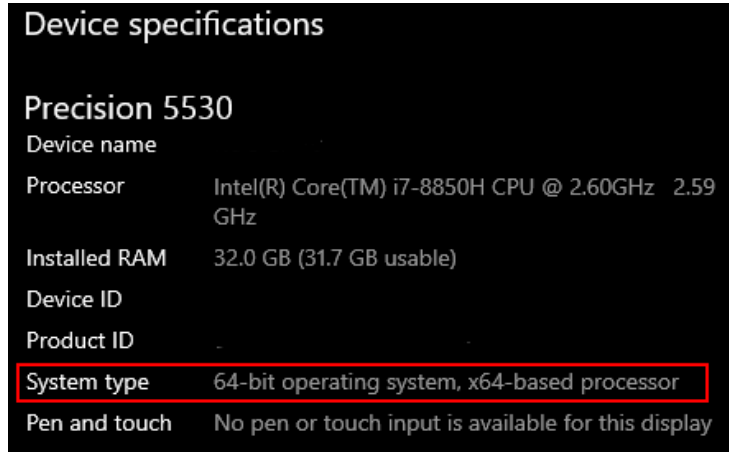


## Windows Installation

The following section describes how to download and install the Cylance agent for Windows.

Complete the following steps to find your Windows 10 Operating System version

On your Windows 10 system, right-click on the Windows Start Icon and select “**Settings**”. Your **System Type** can be found under **Device Specifications**



The screenshot shows the Windows 'Device specifications' window for a Precision 5530. The 'System type' entry is highlighted with a red box, indicating the operating system is 64-bit and the processor is x64-based.

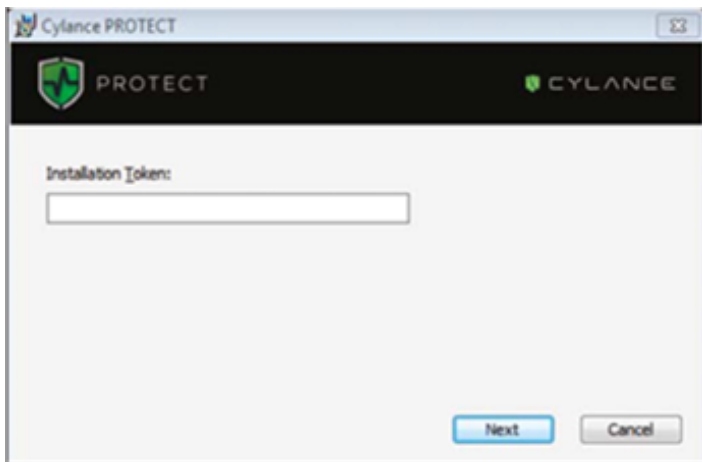
Device specifications	
<b>Precision 5530</b>	
Device name	
Processor	Intel(R) Core(TM) i7-8850H CPU @ 2.60GHz 2.59 GHz
Installed RAM	32.0 GB (31.7 GB usable)
Device ID	
Product ID	
<b>System type</b>	<b>64-bit operating system, x64-based processor</b>
Pen and touch	No pen or touch input is available for this display

If you have existing antivirus software, please add the exclusions below.

<p><b>The following exclusions will need to be proactively added to your existing anti-virus solution to avoid interfering with CylancePROTECT:</b></p>
<p><b>For Windows OS</b></p>
C:\Program Files\Cylance\
C:\Windows\Temp\CylanceDesktopArchive
C:\Windows\Temp\CylanceDesktopRemoteFile
C:\ProgramData\Cylance\Desktop\q
C:\Documents and Settings\All Users\Application Data\Cylance\Desktop\q
Do not scan the following files:
<p><b>For Windows OS</b></p>
C:\Windows\System32\Drivers\CyProtectDrv64.sys
C:\Windows\System32\Drivers\CyProtectDrv32.sys
C:\Windows\System32\Drivers\CyDevFlt64.sys
C:\Windows\System32\Drivers\CyDevFlt32.sys
C:\Windows\CyProtect.cache
C:\Program Files\Cylance\Desktop\CylanceSvc.exe
C:\Program Files\Cylance\Desktop\CylanceUI.exe
C:\Program Files\Cylance\Desktop\CyUpdate.exe
C:\Program Files\Cylance\Desktop\LocalePkg.exe
Add the following processes to the Trusted Programs List:
<p><b>For Windows OS</b></p>
C:\Program Files\Cylance\Desktop\CylanceSvc.exe
C:\Program Files\Cylance\Desktop\CylanceUI.exe
C:\Program Files\Cylance\Desktop\CyUpdate.exe
C:\Program Files\Cylance\Desktop\LocalePkg.exe

## Install the Agent — Windows

1. Double-click CylancePROTECT.exe (or MSI).
2. Click Install at the CylancePROTECT setup window.
3. Enter the Installation Token and click Next



### Installation Token Input Screen

4. Optionally change the destination folder of CylancePROTECT.
5. Click OK to begin the installation.
6. Click Finish to complete the installation. Select the check box to launch CylancePROTECT.

The Agent does not require a reboot when it is installed.

Note: The Agent can run with Windows Defender installed on a device. This requires Agent version 1370 (and higher), a fresh installation of the Agent (not an upgrade), and Windows Defender must be running.

7. Verify successful agent installation.

Check the following files to verify successful Agent installation.

- The program folder was created. Windows default: C:\Program Files\Cylance\Desktop
- The CylancePROTECT icon is visible in the System Tray of the target device. This does not apply if parameter LAUNCHAPP=0 is used.
- There is a CylancePROTECT folder under Start Menu\All Programs on the target device. This does not apply if parameter LAUNCHAPP=0 is used.
- The CylancePROTECT service was added and is running. There should be a CylancePROTECT service listed as running in the Windows Services panel of the target device.

- The CylanceUI.exe process is running. There should be a CylanceUI.exe process listed under the Processes tab in the Windows Task Manager of the target device.
- The device is reporting to the Console. Login to the console and click the Devices tab. The target device should show up and be listed in the online state.

## MacOS Installation

The following section describes how to download and install the Cylance agent for MacOS.

If you have existing antivirus software, please add the exclusions below.

**The following exclusions will need to be proactively added to your existing anti-virus solution to avoid interfering with CylancePROTECT:**

**For Mac OS**

/Library/Application Support/Cylance/Desktop/q

/Library/Application Support/Cylance/

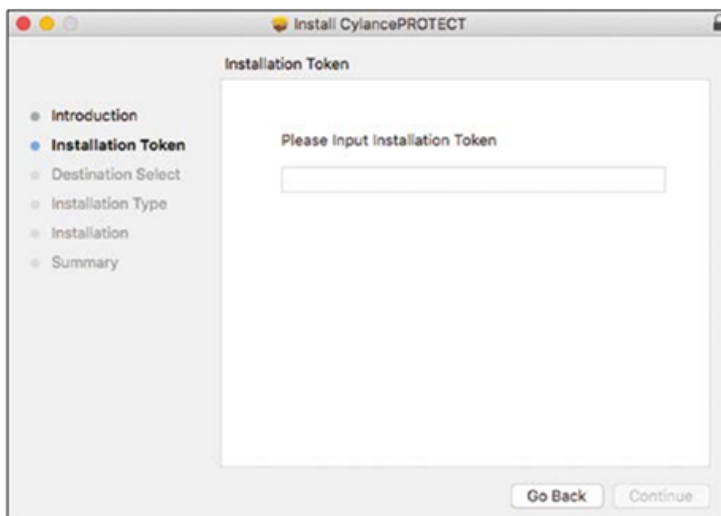
/System/Library/Extensions/CyProtectDrvOSX.kext/

/private/tmp/CylanceDesktopArchive

/private/tmp/CylanceDesktopRemoteFile

### Install the Agent — mac

1. Double-click the CylancePROTECT.dmg (or .pkg) to mount the installer.
2. Double-click the Protect icon from the PROTECT user interface to begin the installation.
3. Click Continue to verify that the Operating System and Hardware meet the requirements.
4. Click Continue at the Introduction screen.
5. Enter or copy/paste the Installation Token provided by the Tenant. Click Continue. The Destination Folder step displays.



Installation Token Input Screen



6. Optionally change the installation location of CylancePROTECT.
7. Click Install to begin the installation.
8. Enter an administrator's Username and Password. Click Install Software.
9. Click Close at the Summary screen.
10. Click OK. When installation is done, the Completed step displays.
11. Click Finish.

### macOS High Sierra – Secure Kernel Extension Loading

macOS High Sierra (10.13) includes a security feature that requires users to approve new third party kernel extensions. This security feature only allows kernel extensions to load on a system that is already approved by the user. If an unapproved extension tries to load, the extension is blocked and displays a user alert.

If the Agent is installed without approving the extension, the Cylance icon displays a red dot. Clicking on the icon and selecting Show Details, displays the message "Driver Failed to Connect, Device Not Protected" at the bottom.

Note: This only affects new Agent installations on macOS High Sierra. This will not affect Agents installed on macOS devices that were then upgraded to macOS High Sierra.

1. When installing the Agent on macOS High Sierra for the first time, a user alert displays.




macOS User Alert

2. To approve the extension, click Open Security Preferences, or go to System Preferences > Security & Privacy.
3. Click Allow. Clicking the Allow button does not work over a Remote Desktop session. This is by design by Apple.



Allow the Agent to Install

#### macOS Installation Verification

4. Check the following files to verify successful Agent installation.
  - The program folder was created. macOS default: /Applications/Cylance/
  - The CylancePROTECT icon is visible in the System Tray of the target device. 
  - This does not apply if parameter NoCylanceUI is used.
  - The CylanceSvc is running in the Activity Monitor of the target device or use Terminal (eg. "ps -ax | grep -i cylance").
  - The Cylance logs are being generated and tracing out. The logs are located in the following location: /Library/Application Support/Cylance/Desktop/log
  - The device is reporting to the Console. Login to the console and click on the Devices tab. The target device should show up and be listed in the online state.

## Minimum Requirements

The following section describes how to download and install the Cylance agent for MacOS.

MicroSoft Windows (32-bit or 64-bit)	Mac OS	Linux
<ul style="list-style-type: none"> <li>• Windows XP SP3</li> <li>• Windows Vista</li> <li>• Windows 7</li> <li>• Windows 8 and 8.1</li> <li>• Windows 10</li> <li>• Windows Server 2003 SP2</li> <li>• Windows Server 2008 / 2008 R2</li> <li>• Windows Server 2012 / 2012 R2</li> <li>• Windows Server 2016</li> </ul>	<ul style="list-style-type: none"> <li>• Mac OS X 10.9 (Mavericks)*</li> <li>• Mac OS X 10.10 (Yosemite)*</li> <li>• Mac OS X 10.11 (El Capitan)*</li> <li>• Mac OS X 10.12 (Sierra)*</li> </ul>	<ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux / CentOS 6.6 — 32-bit and 64-bit</li> <li>• Red Hat Enterprise Linux / CentOS 6.7 — 32-bit and 64-bit</li> <li>• Red Hat Enterprise Linux / CentOS 6.8 — 32-bit and 64-bit</li> <li>• Red Hat Enterprise Linux / CentOS 7.0 — 64-bit</li> <li>• Red Hat Enterprise Linux / CentOS 7.1 — 64-bit</li> <li>• Red Hat Enterprise Linux / CentOS 7.2 — 64-bit</li> <li>• Red Hat Enterprise Linux / CentOS 7.3 — 64-bit</li> </ul>
Requirements	Requirements	Requirements
<ul style="list-style-type: none"> <li>• 2GB Memory</li> <li>• 500MB Available Disk Space</li> <li>• Microsoft .NET Framework 3.5 SP1</li> <li>• Internet browser</li> <li>• Internet connection to register product</li> <li>• Local admin rights to install software</li> </ul>	<ul style="list-style-type: none"> <li>• 2GB Memory</li> <li>• 500MB Available Disk Space</li> <li>• Internet browser</li> <li>• Internet connection to register product</li> <li>• Local admin rights to install software</li> </ul>	<ul style="list-style-type: none"> <li>• 2GB Memory</li> <li>• 500MB Available Disk Space</li> <li>• Internet browser</li> <li>• Internet connection to register product</li> <li>• Local admin rights to install software</li> </ul>