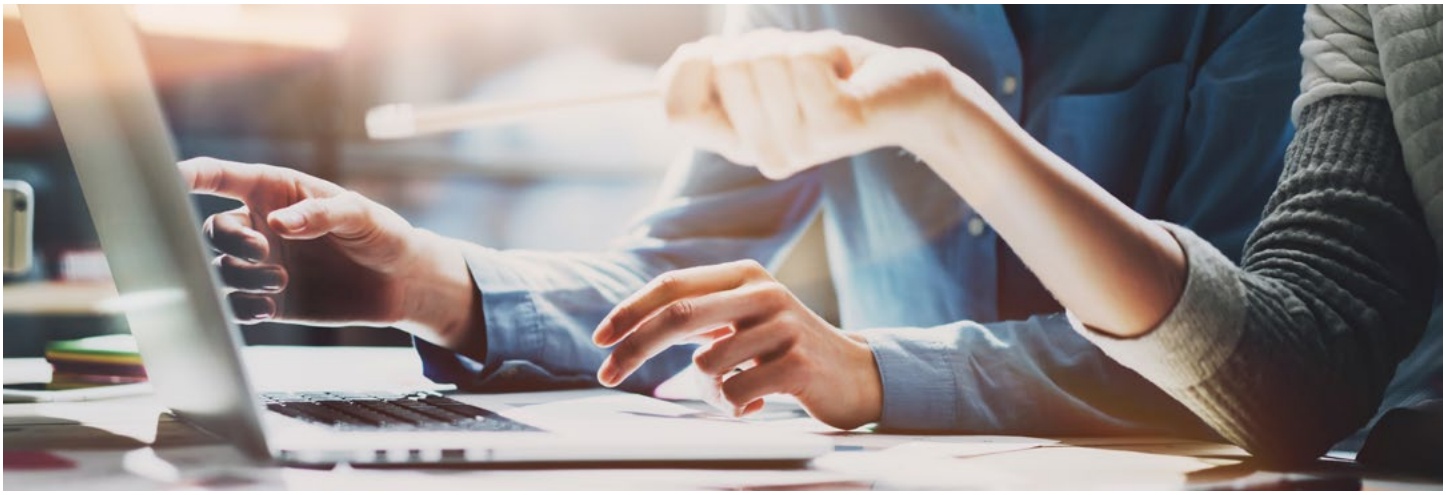
Fast Incident Response with CylanceOPTICS™

Feature Focus

CYLANCE™



Incident Response

Identifying a potential security issue in your environment is important, however to protect your business from the fallout of a widespread successful attack, you need the ability to respond fast.

With CylanceOPTICS, you have several built-in incident response options that enable you to take action as soon as you determine that a process, executable, file, or endpoint may be harmful to your environment.

Response Options:

- **Download the suspicious file —** With a single click, you can download any suspicious file you encounter to complete a deeper investigation with third-party tools
- **Globally quarantine the item —** If an item is determined to be malicious based on your investigation, you can easily add the item to the Global Quarantine list, restricting any endpoint in your environment from interacting with the item
- **Lockdown the endpoint —** If an endpoint is determined to be the source of an outbreak or has been identified as harmful to your environment for some reason, you can take an aggressive containment move and lock down the endpoint, eliminating its ability to connect to your network

With these capabilities, you can complete your investigations to detect potential security issues and take steps to stem the attack, protect your sensitive data, and keep your business secure.

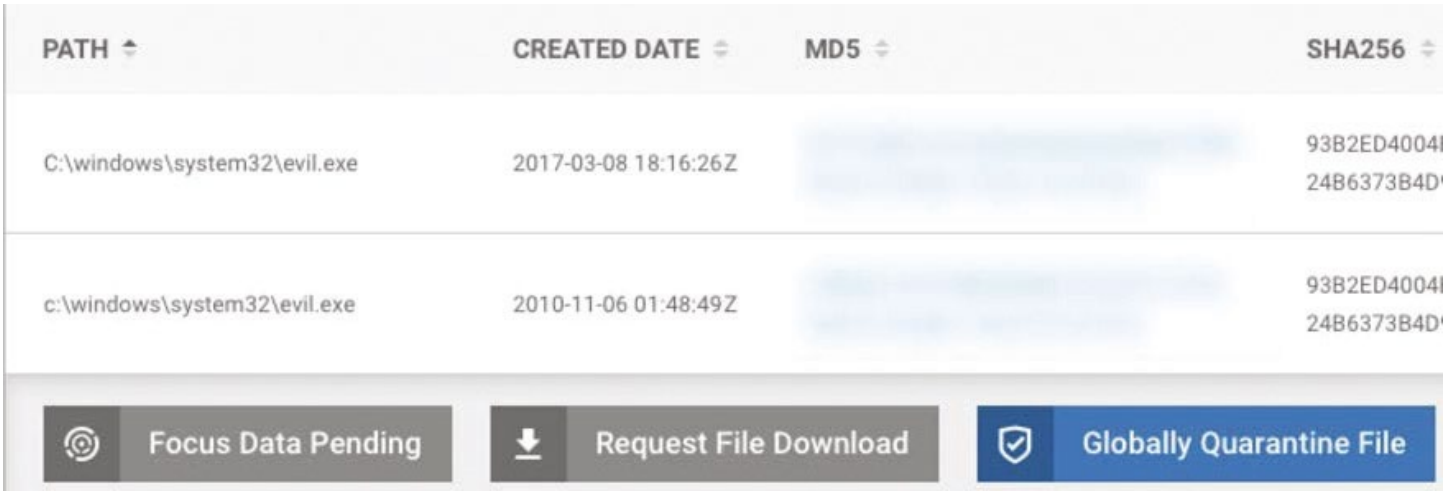
Technical Details Summary

Download the Suspicious File

Any file can be downloaded from an InstaQuery results page. If path information is available for files associated with other artifact types, those files can also be retrieved. The file is compressed and password-protected to ensure it is not accidentally executed. This action is only available to administrators in the Cylance Console.

A successful download file request displays a **Download File** button. The file may be unavailable if the device is offline, or the file is removed from the device.

The file size limit for retrieval is 50MB.



Response Options

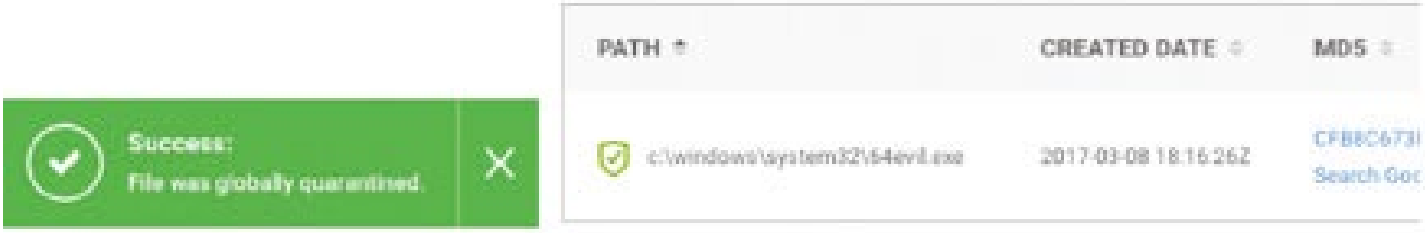
Globally Quarantine the Item

From an InstaQuery, you can globally quarantine a file. This action is only available to administrators in the Cylance Console.

1. From the InstaQuery Results page, click the **Actions** menu.
2. Select **Global Quarantine**, type in a reason for quarantining the file, then click **Confirm Quarantine**.

Successful global quarantine of a file displays a pop-up and an icon in the Path column. Hovering over the icon displays the file status as globally quarantined. If an error occurs, an error pop-up displays, and the quarantined icon does not display in the Path column.

This file will now be visible in the **Global List > Global Quarantine** section of the console, and – if executed – will show up as a threat in the Protection page and the Threats section of the Device Details page.



File Quarantined

Lockdown the Endpoint

With CylanceOPTICS, administrators can quickly isolate an infected (or potentially infected) device to stop command and control (C2) activity, exfiltration of data, or lateral movement of malware. The lockdown feature gives administrators time to investigate the device or physically remove the device from the network. This action is only available to administrators in the Cylance Console.

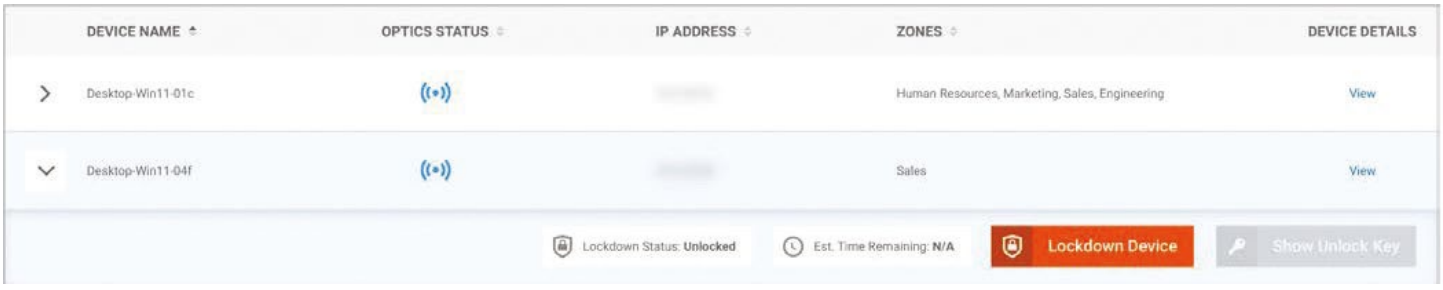
Lockdown disables the network capabilities of the device (LAN and Wi-Fi) for a period of time, from five minutes to 96 hours. If desired, the device can be unlocked prior to the selected lockdown end time using the unlock key.

About Lockdown

- When an endpoint lockdown time has expired, it can take up to two minutes for that device to appear as connected on the Devices page in CylanceOPTICS
- CylancePROTECT® Agent 1440 and above will display a message on the endpoint (via a notification) when it has been placed into a lockdown

Once a device has been locked down, the status column will show a red icon in the CylanceOPTICS column to indicate a device is in lockdown.

A lockdown can also be initiated from any InstaQuery result, which will re-direct to the devices page filtered to the device associated with the artifact.



Lockdown Option

Lockdown Options

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