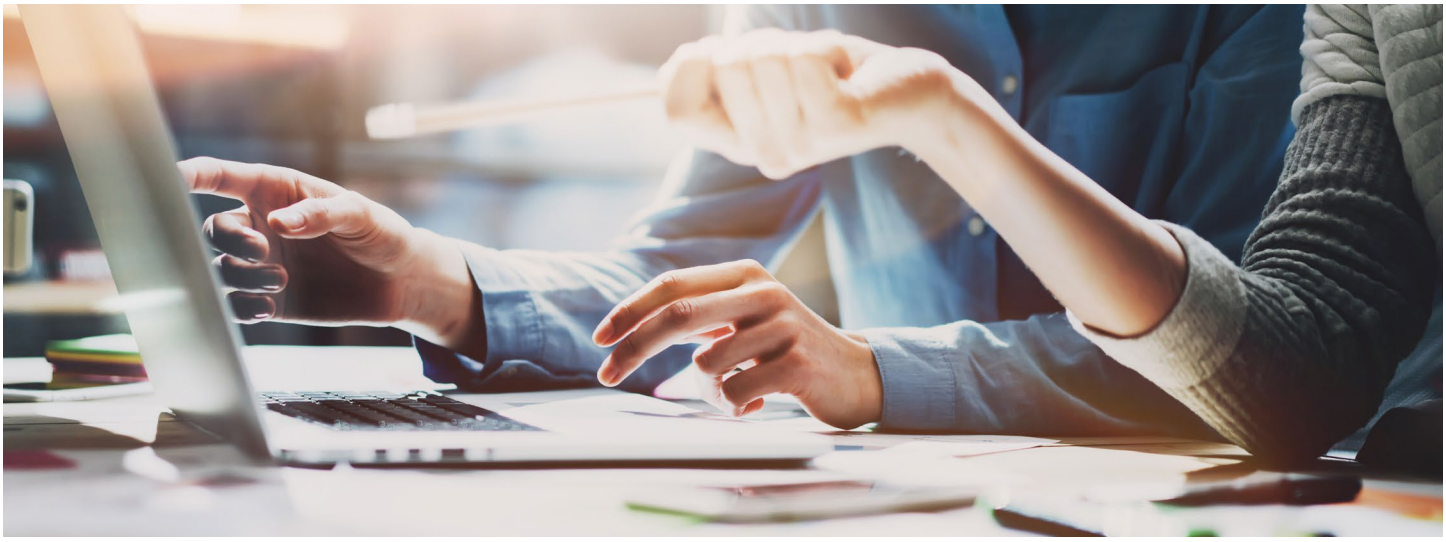
Fast Incident Investigation and Response with CylanceOPTICS™

Feature Focus

CYLANCE



Incident Investigation and Response

Identifying a potential security issue in any environment is important, however, to protect from the fallout of a widespread incident, businesses need the ability to investigate and respond to an attack fast.

With CylanceOPTICS, businesses get several built-in incident investigation and response options that enable them to gather relevant information about an incident and act fast, either in automated or manual fashion.

Investigation Options:

- **Remote Forensic Data Collection:** Using the built in hardened Python interpreter and a proprietary communication protocol optimized for speed and scalability, users can interact with endpoints across the organization in near real time, gathering critical incident related data. In addition to data collection, users can initiate other endpoint tasks such as third-party scripts and applications, as well as take custom remediation actions, all without ever touching the keyboard of the remote machine.
- **Root Cause Analysis:** Anytime a confirmed or suspected threat is uncovered, analysts can dissect the potential attack, looking for signs of the tactics, tools, and procedures the attacker used to carry out the attack and identifying weaknesses in their security framework.
- **Enterprise-Wide Threat Hunting:** At times, an initial attack may only be a diversion from the actual objectives of the adversary. Using information collected about the potential incident, analysts can carry out streamlined, targeted searches across the business, looking for other signs of compromise.

Automated Response Options:

- **Context Analysis Engine (CAE) Rules: Behavior Based Static Rule Automated Response:** Cylance's CAE automates threat discovery and response, in real time, allowing users to configure custom behavior based rules and/or enable the Cylance-curated detection rules to prevent attackers from reaching their goal.
- **Context Analysis Engine Rules: Machine Learning Threat Detection Module Automated Response:** Machine Learning Threat Detection Modules continuously analyze changes occurring on each endpoint to uncover threats that would be difficult, if not impossible, for a human analyst to uncover in a reasonable amount of time. When a potential threat is identified, Cylance's CAE can take decisive actions, in real time, to stop the attack and avoid the cost, risk, and long-term impacts that come with a widespread security incident.

Manual Response Options:

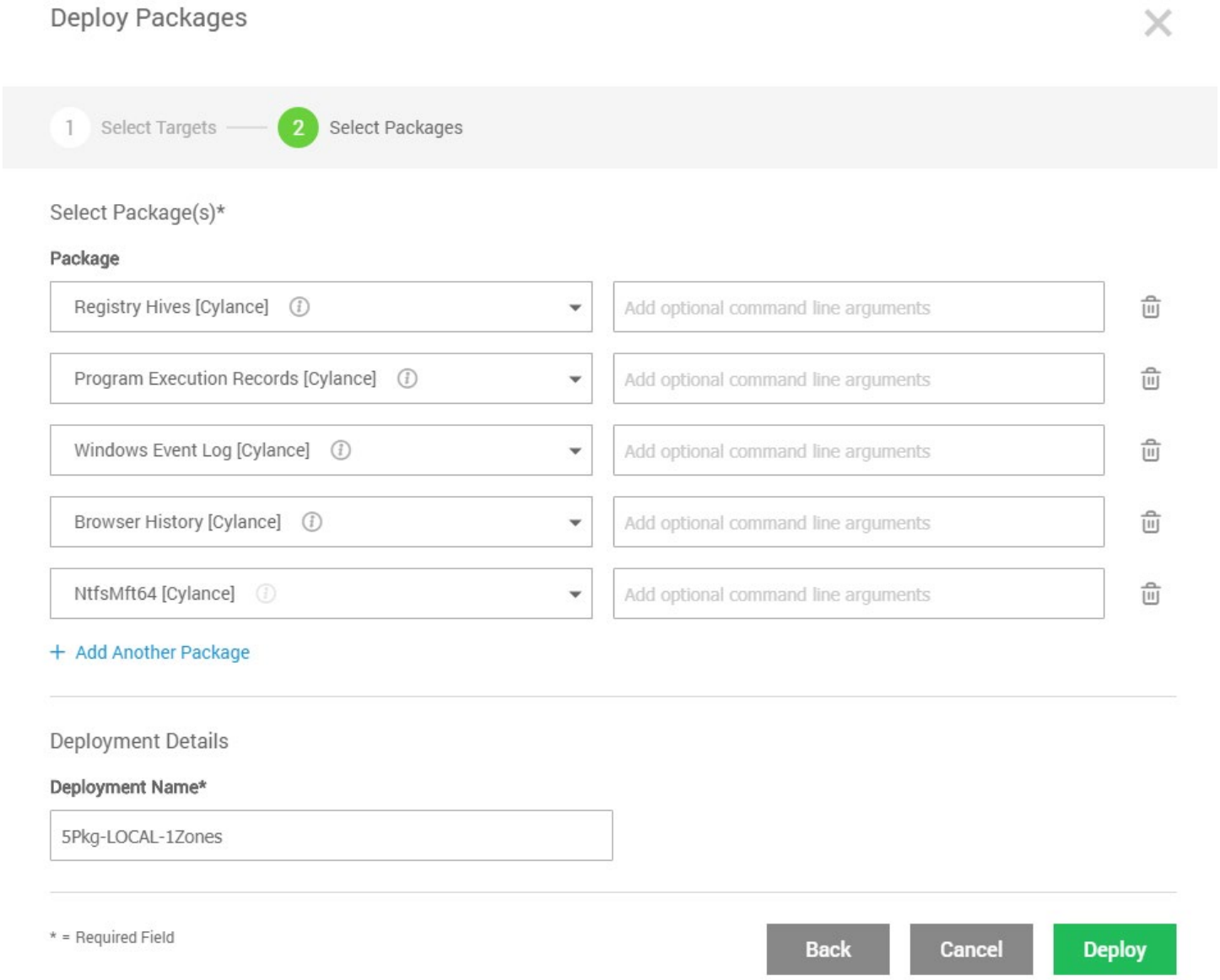
- **Download the Suspicious File:** With a single click, any suspicious file encountered can be downloaded to complete a deeper investigation with third-party tools.
- **Globally Quarantine the Item:** If an item is determined to be malicious upon investigation, it can easily be added to the Global Quarantine list, restricting any endpoint in the 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 the environment for some reason, aggressive containment can be taken to move and lock down the endpoint, eliminating its ability to connect to the network.

With these capabilities, potential security issues can be detected quickly and the necessary steps can be taken to stem the attack, protect sensitive data, and keep the business secure.

Technical Details Summary

Investigation Options

Remote Forensic Data Collection



CylanceOPTICS Remote Forensic Data Collection utilizes a hardened Python interpreter packaged with the CylanceOPTICS service on each endpoint coupled with the speed of the CEMENT communications channel to provide near real-time interactions with endpoints throughout an organization. This feature allows users to access endpoints running CylanceOPTICS in a programmatic manner to conduct various operations, including:

- Forensic artifact retrieval
- Execution of third-party scripts and applications
- Custom security incident remediation

While users will be able to accomplish many of their tasks using only Python code, it is possible to utilize various methods within Python, such as the subprocess library, to execute other scripting languages or applications.

Viewing Packages

A list of currently available Packages to each tenant is available via Configurations -> Packages. On this page, users will find a list that includes the Package's name, a tooltip of the Package's description, the main file the Package executes, the size of the Package, when it was uploaded, and who uploaded the Package.

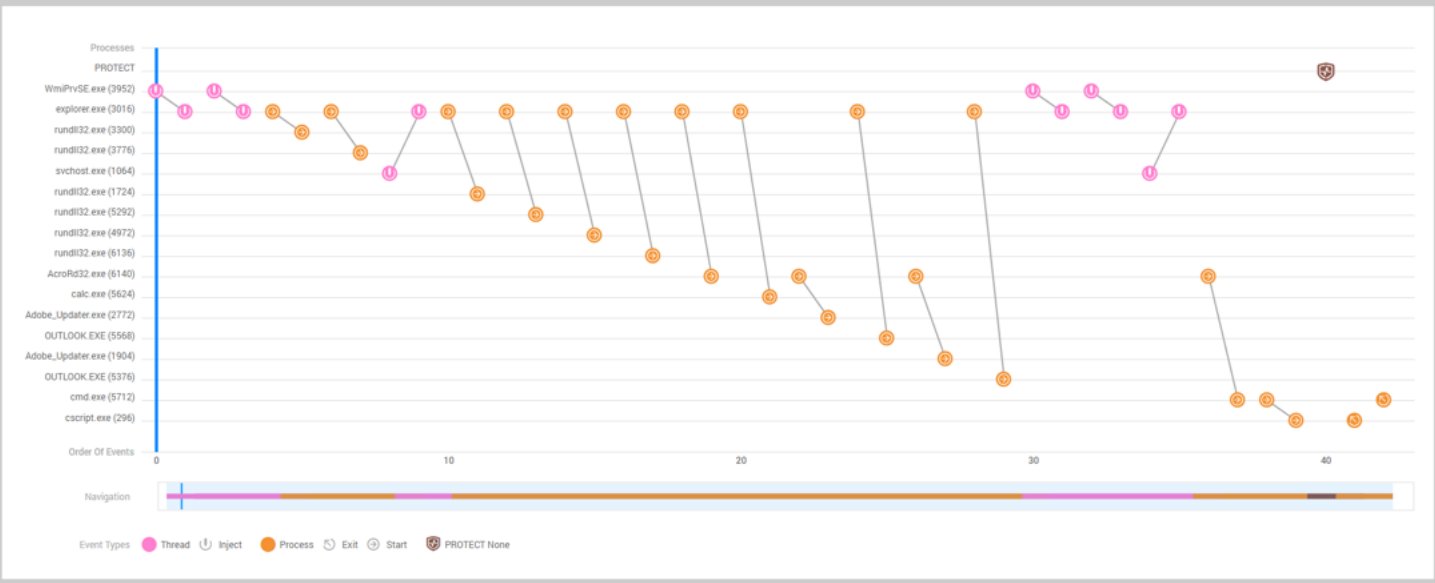
Uploading Packages

Users can upload Custom Packages by clicking the Upload File button. The menu displayed notes that Packages must be a .zip archive and cannot be larger than 15MB in size. To create a valid Package that can be uploaded and interpreted by CylanceOPTICS endpoints.

Hosts File Collection

One of the primary use cases of the Remote Forensic Data Collection feature is to collect raw forensic artifacts from systems of interest for additional analysis by security staff. While the default packages provided by Cylance® have the capabilities to collect some common artifacts, users may be interested in obtaining additional data from systems that they deem to be of interest.

Root Cause Analysis



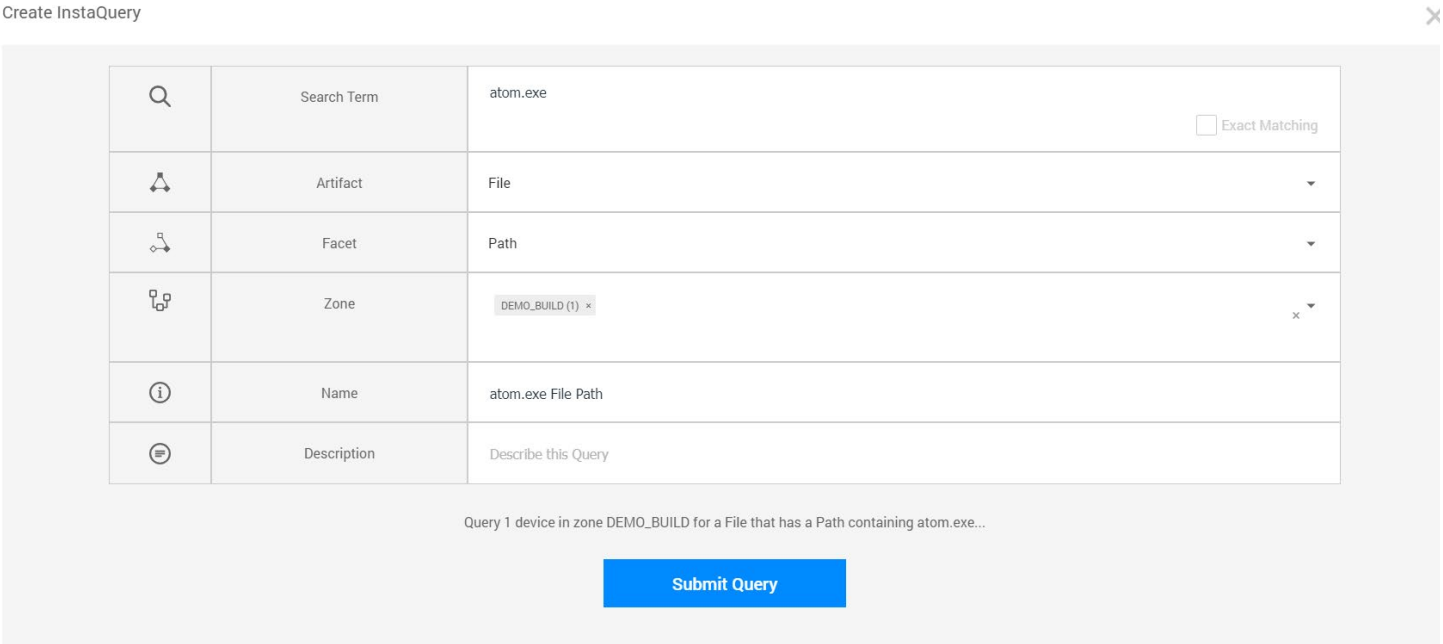
Viewing Focus Data

Focus Data provides an information trail starting with the first event related to an artifact from an InstaQuery result or a CylancePROTECT® event.

There are multiple ways to view Focus Data. The Focus Data tab on the CylanceOPTICS page shows a table of previously requested Focus Views from InstaQuery searches, and CylancePROTECT events. If Auto-Focus is not enabled, Focus Views for CylancePROTECT events must be requested from the Device Details page under Threats and Activities. The time for CylanceOPTICS to return Focus View results is directly proportional to the size of the data being queried. More generic queries will take longer to return results. This is also dependent on the network traffic and bandwidth on the network.

If Auto-Focus is enabled in the policy associated with a device, the View Data link in the Focus View column will link to the Focus View for the most recent threat. In cases where these detonations take place over multiple minutes, Focus Views from these previous threats are visible in the Focus Data tab in CylanceOPTICS.

Enterprise-Wide Threat Hunting



In CylanceOPTICS, users can complete enterprise-wide threat hunts via the InstaQuery (IQ) tab for:

- Files
- Registry Keys
- Processes
- Network Connections

Upon initiating the search, CylanceOPTICS will query the selected endpoints for the information requested, interrogating the data stored on the endpoints and collecting all responsive items. The results of the IQ search are stored in the cloud so that they can be easily referenced in the future.

Once a query has reached completion, the user can review the results in a table format or, for targeted searches, use the facet breakdown view to drill into the results of the query. This simple interrogation of endpoint data means that anyone, regardless of skill level, can gain insights into endpoint activity in a matter of minutes.

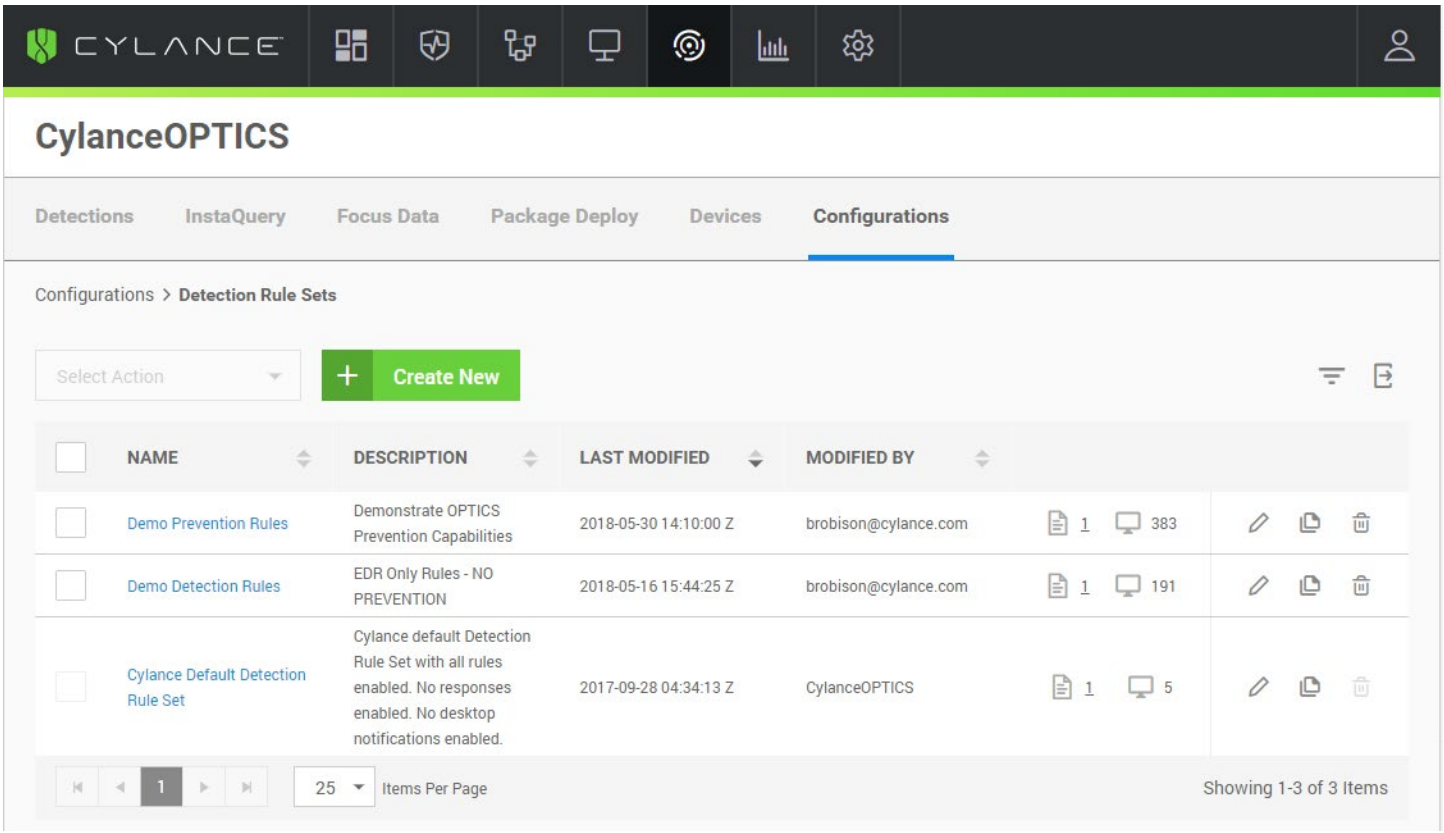
Response Options

CAE: Behavior Based Static Rule Automated Response

To address the need for automated real-time threat detection and response issues, Cylance has developed a new approach to threat detection and response, known as the Context Analysis Engine, which runs on the endpoint and eliminates the latency issue that plagues other EDR products. Now, every endpoint in an organization acts as its own virtual security operations center with the ability to dynamically detect threats and take response actions without human intervention, around the clock. Security teams can now focus on investigating advanced threats, improving overall security infrastructure, or any other business-critical project, with the confidence that the CylanceOPTICS Context Analysis Engine is working to keep the endpoint, and the business, secure.

Configuring the CAE

The CAE is a rules engine that runs local on every endpoint in the environment. Upon deploying CylanceOPTICS, the user can configure a set of behavior rules, either custom or Cylance-curated rules, that will ultimately be pushed down to each endpoint. The flow of response will be the same for both behavior rules and the machine learning threat detection module rules that are explained in the next section. These behavior rules will continuously monitor the data collected and stored locally on the endpoint. When a detection rule is triggered, a response action can be taken automatically.



CAE: Machine Learning Threat Detection Module Automated Response

Unlike EDRs based on behavior rules, which require a person to write, maintain, and continually add rules that are essentially behavior signatures to trap single attacks, Cylance's AI Incident Prevention can render an entire class of attacks useless. A single model, specifically trained to identify a specific attack class or TTP can be deployed on an endpoint, essentially eliminating the need for the hundreds or thousands of behavior rules a security analyst would have to create and maintain to deliver comparable protection.

This first release of AI models for threat detection and incident prevention will target the following specific attack types:

- **Fileless Attacks:** So-called fileless attacks may be fileless in the sense that they do not rely on a malicious or suspicious binary; however, they will typically rely on other system-based artifacts that can be easily sensed and correlated with CylanceOPTICS. The Fileless Attack Model evaluates the context and parameters of system utility invocations to understand their intended outcomes.
- **Malicious or Suspicious One-Liner Commands:** Scripting engines like CMD, PowerShell, and Wscript are the workhorses of IT operations, but they expose a significant amount of functionality that can be leveraged by malicious actors. This malicious or suspicious usage becomes increasingly more difficult to detect when multiple actions are strung together and hidden behind varying layers of obfuscation, whether it be encoding or abuse of environment variables, whitespace, and other characters. The Malicious One-Liner Model evaluates the content of command line scripts with an emphasis on the language of the script and the command line context of the script.
- **Malicious Application Behavior:** An overwhelming number of attacks target a small, predictable number of trusted applications commonly found in enterprise environments. The Malicious Application Behavior Model learns legitimate interactions between common software and the operating system, and blocks anything that veers too far off course.

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.

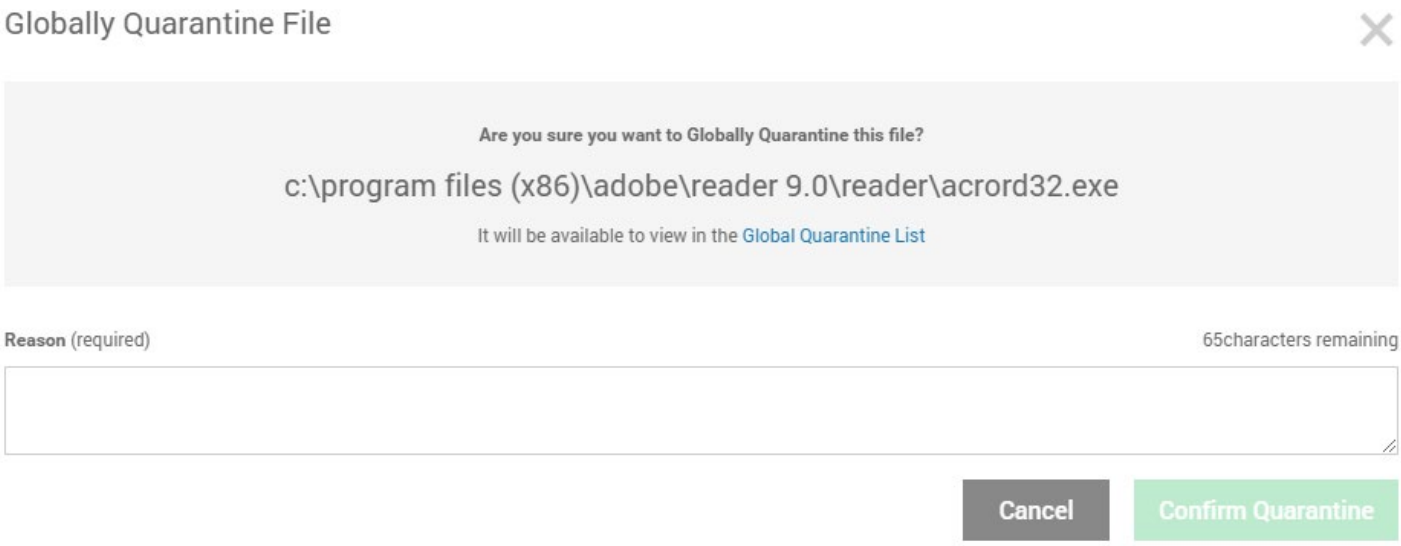
A successful download file request displays a Download File button. The file may be unavailable if the device is offline, or the file is removed from the device.

The file size limit for retrieval is 50MB.

Globally Quarantine the Item

From an InstaQuery, a file can be globally quarantined. 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**.

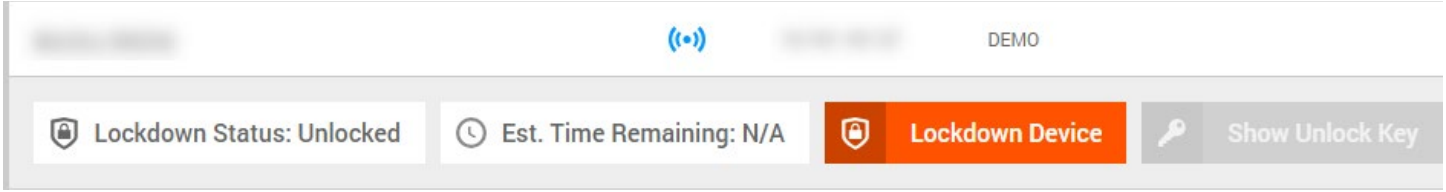


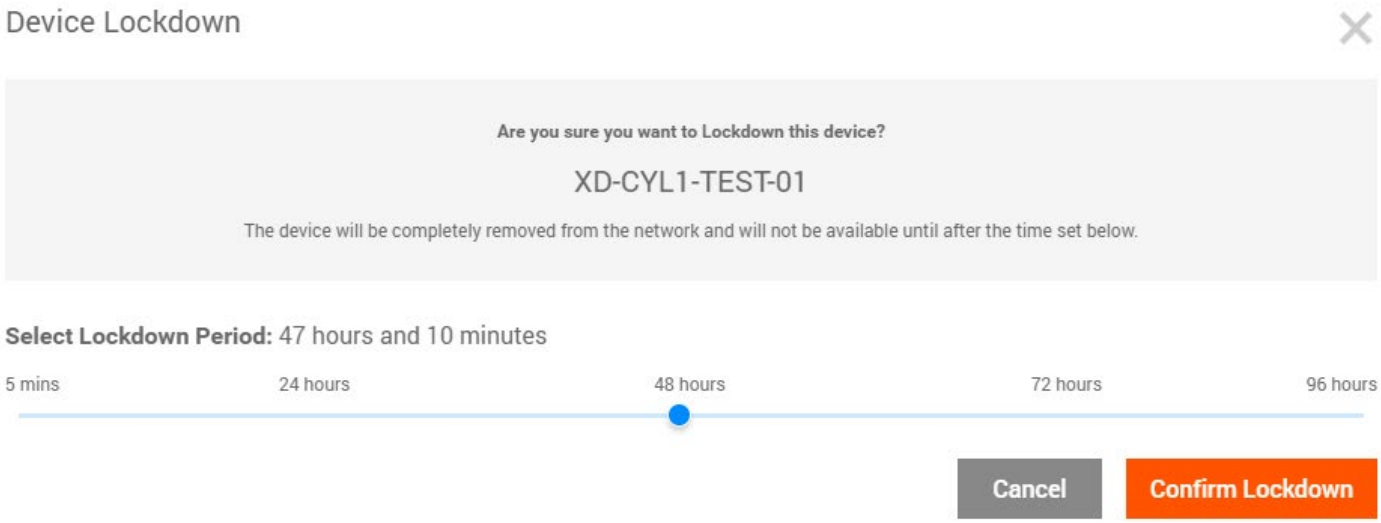
Successful global quarantine of a file displays a pop-up and an icon in the Path column. Hovering over the icon displays the file status as globally quarantined. If an error occurs, an error pop-up displays, and the quarantined icon does not display in the Path column. This file will now be visible in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

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.

+1-844-CYLANCE
sales@cylance.com
www.cylance.com
400 Spectrum Center Drive, Irvine, CA 92618