Root Cause Analysis with CylanceOPTICS™

Feature Focus

CYLANCE™

Root Cause Analysis

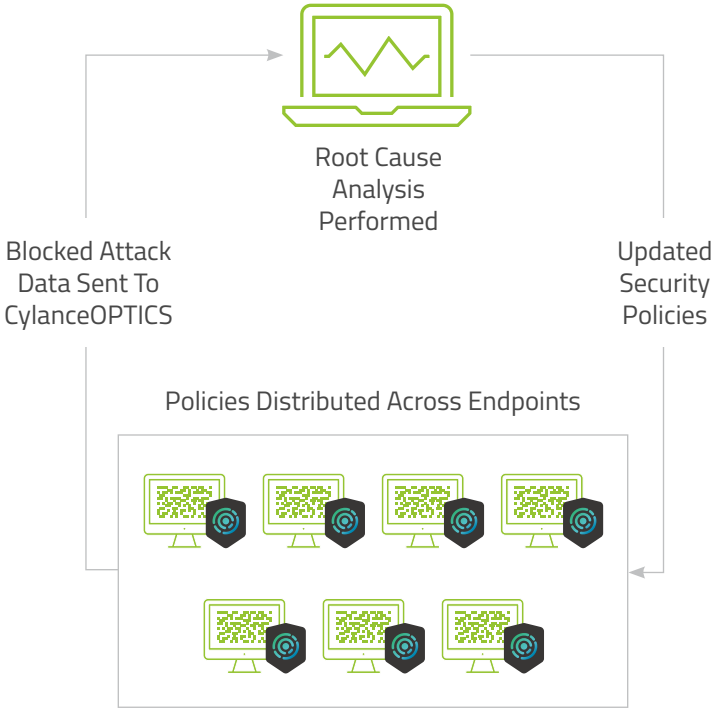
CylancePROTECT® prevents known and unknown threats from executing on your endpoints, as well as from attackers attempting to exploit memory, detonate malicious scripts, or use external devices to compromise an endpoint.

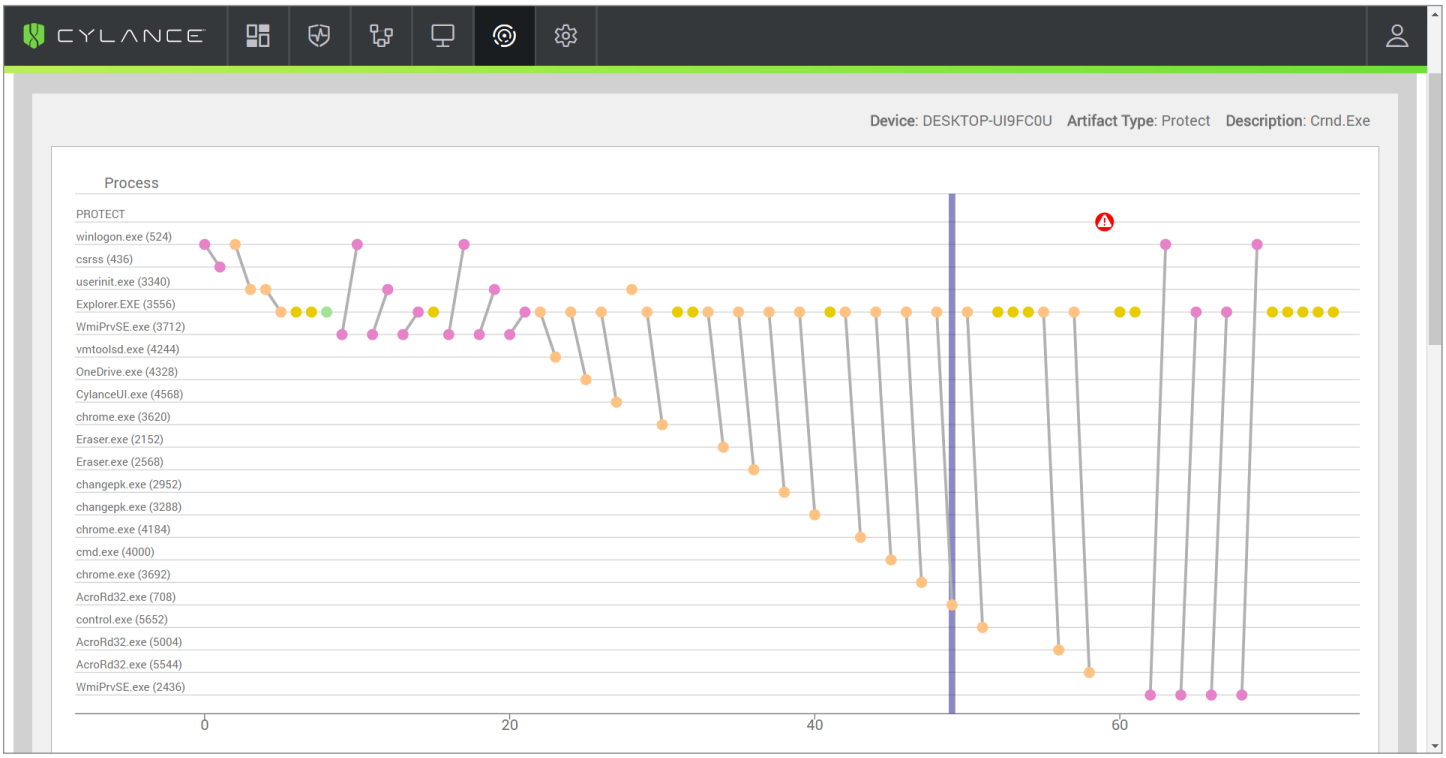
With the addition of CylanceOPTICS' ability to perform on-demand root cause analysis, you can now make use of the blocked attack data to improve your overall security posture.

When CylancePROTECT blocks a malicious executable, memory or script attack, or a corrupt USB device, CylanceOPTICS will gather a set of data associated with the event. That event data will then be sent to the cloud-based web console for a security analyst to perform root cause analysis using the Focus View feature.

The Focus View is a recreation of the events associated with the blocked event that displays the relationship between each event.

Within Focus View, there are three different ways to interact with the data: 1) Graphical view, 2) Event Card view, and 3) Tabular view.





1) Graphical View: *As you click on a dot (which represents an activity), the corresponding event card is brought into focus.*

Filter Term | Search | Export Results

TIME	CATEGORY	SUBCATEGORY	TYPE	PATH	PARENTID	PROCESSID
2017-04-18T00:29:26.681Z	Process		Start		11076	2948
2017-04-18T00:29:26.681Z	Process		Started		11076	2948
2017-04-18T00:29:26.706Z	Memory	PROTECT	StackProtect		11076	2948
2017-04-18T00:29:26.721Z	Process		Normal Exit		11076	2948

1 10 Items per page

2) Event Card View: *With this detailed view into a CylancePROTECT blocked event, analysts can adjust their security controls, close vulnerabilities, and improve their overall security framework to ultimately reduce their attack surface.*

EXPLORER.EXE (PROCESS - START)

ProcessId 5652
Name control.exe
CommandLine "C:\Windows\system32\control.exe"/name Microsoft.DefaultPrograms
EndDateTime 2017-04-26T05:57:39.597Z
StartDateTime 2017-04-26T05:57:39.358Z
ParentId 3556
Description Windows Control Panel
OccurrenceTime 2017-04-26T05:57:39.347Z

CONTROL.EXE (PROCESS - STARTED)

ProcessId 5652
Name control.exe
CommandLine "C:\Windows\system32\control.exe"/name Microsoft.DefaultPrograms
EndDateTime 2017-04-26T05:57:39.597Z
StartDateTime 2017-04-26T05:57:39.358Z
ParentId 3556
Description Windows Control Panel
OccurrenceTime 2017-04-26T05:57:39.347Z

NETWORK - CONNECT

Source 192.168.241.190:50428
Destination 23.7.139.27:80
OccurrenceTime 2017-04-26T05:57:44.831Z

3) Tabular View: *From the tabular view, you can choose to export the event list and complete your root cause analysis using other tools.*

Technical Details Summary

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.

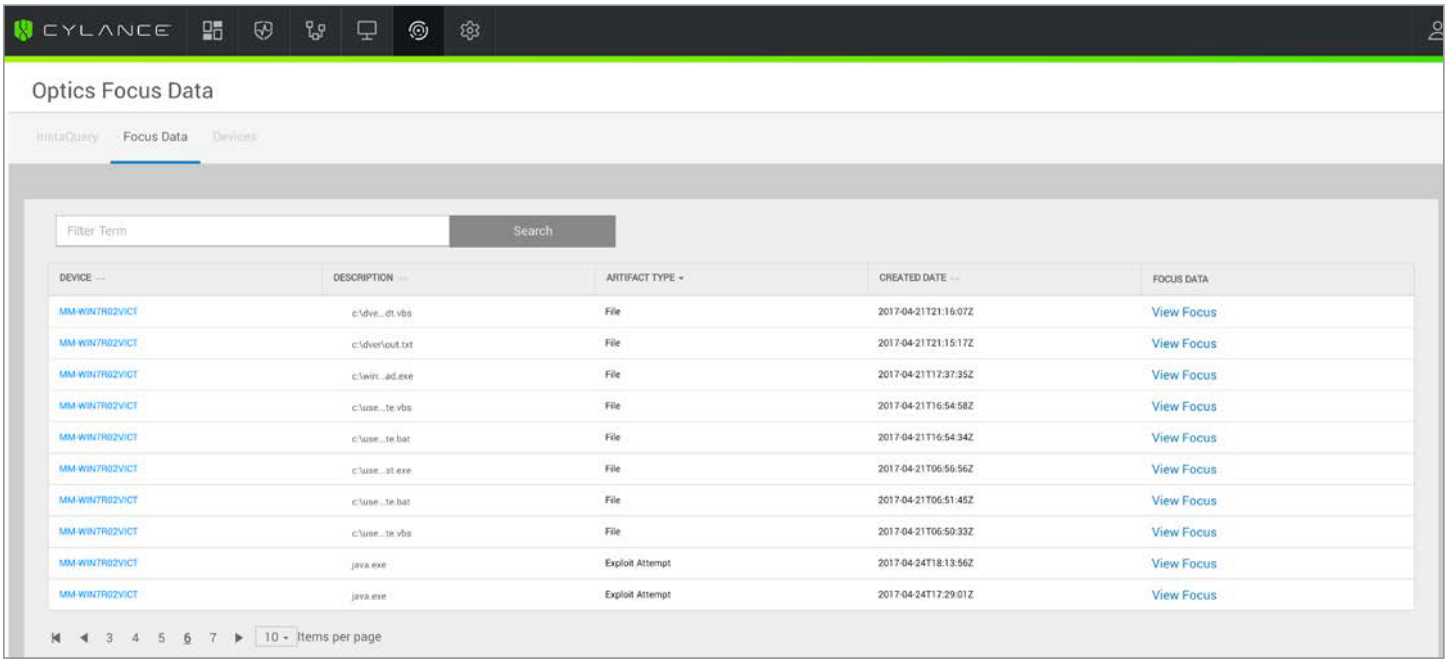
There are multiple ways to view Focus Data. The Focus Data tab on the CylanceOPTICS page shows a table of previously requested Focus Views from InstaQuery searches, and CylancePROTECT events. If auto-focus is not enabled, Focus Views for CylancePROTECT events must be requested from the Device Details page under Threats and Activates (see next page).

> **NOTE:** *Data retention span is 30 days for CylanceOPTICS data, including the Download History.*

About Focus Data:

- 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 customer's 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.

Focus Data	Description
Device	The name of the device associated with the Focus View
Description	Facet value of the query, the name of the associated file from an exploit attempt, or the path for a threat
Artifact Type	The artifact from either the InstaQuery search or the CylancePROTECT event
Created Date	The date on which the Focus View was requested.
Focus Data	The link to view the Focus View data



Available Focus Views.

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

20170519-0999