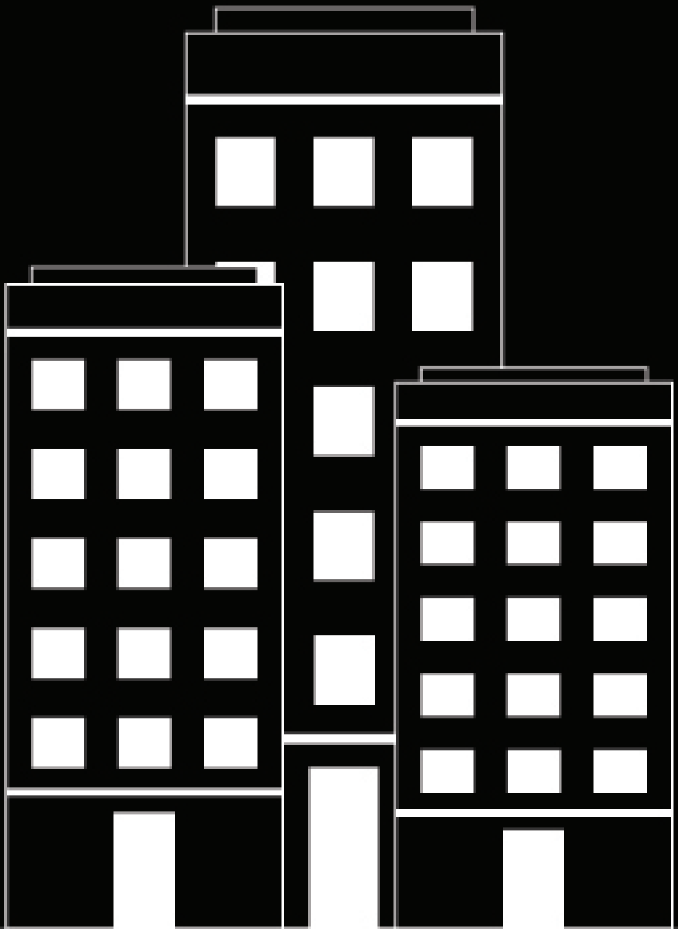


BlackBerry Optics

Administration Guide

2.5.3010

Contents

What is CylanceOPTICS?

CylanceOPTICS operates by deploying sensors into the endpoint's operating system at various levels and against various subsystems to collect a diverse set of information and then aggregates that information into a localized data store to track, alert upon, and respond to complex malicious situations as they unfold. CylanceOPTICS connects to a cloud-based analytics backend infrastructure through a lightweight communications network that enables users, using the Cylance Console, to command and query CylanceOPTICS in real time, against their local data store of forensic data.

CylanceOPTICS consists of the following components.

Component	Description
Endpoint Service - integrated with the endpoint agent of CylancePROTECT	The Endpoint Service is a .NET/Mono 4.5 service with native and managed sensors that observe, interpret, catalog, and provide interfaces into endpoint events.
Communication Network	The Communication Network is a mesh-like network bridging thousands of endpoints together with a communication management framework, delivering real time interaction and awareness.
Data Analytics Backend	The Data Analytics Backend is a highly scalable backend that delivers rich interpretations of endpoint data, as well as an API-first approach to endpoint management.
CylanceOPTICS Microsite in Management Console	The CylanceOPTICS microsite is an ever-evolving front-end delivering powerful views and capabilities from inside endpoints directly to security professionals.

Architecture overview

Architecture	Description
Enterprise Endpoints and Endpoint Architecture	When CylanceOPTICS is installed, sensors are deployed to collect system-level events that are transformed and stored locally on the endpoint. Any events that take place after CylanceOPTICS is installed can have commands executed against it (see below).
Commands and Policies	From the console, users can investigate and issue commands to perform actions on the endpoints. Examples of this include returning query results from the endpoint database through InstaQuery or Focus Views. Commands can also be issued to take actions on that endpoint, like returning a file to the console for analysis or locking down a device from all network activity.
CylanceOPTICS Data	The device sends requested data to the AI engine, which dynamically scales to perform aggregation, enrichment, and correlation.

How it works

CylanceOPTICS is installed alongside CylancePROTECT on each endpoint and is controlled and managed from within the same console.

- CylanceOPTICS will store forensically pertinent data in a secure database on each endpoint locally.
- This data is retrieved on-demand through performing what is known as an InstaQuery (IQ) or uploaded automatically when a CylancePROTECT event occurs, depending upon policy settings.
- The data is then correlated and ultimately presented as focus views within the console. Focus views contain the correlated chain of events displayed visually as well as in full detail.
- Additional remediation actions can be taken on endpoints based upon the results returned from an IQ or focus view.

CylanceOPTICS stores, retrieves, correlates, and presents the following artifacts and supporting details.

Artifact	Description
DNS	When a domain resolution is requested and answered
File	When non-empty files are created, modified, deleted, or renamed
Network	Information about IP addresses, ports, and associated events
Powershell	When a Powershell command or script is executed
Process	When processes are created or modified
Registry	Alterations to the Windows registry surrounding persistent events
Thread	When processes are injected or spawned from another process
Windows Events	When specific security-relevant Windows Events occur
WMI	When the Windows Management Instrumentation (WMI) queries are executed

Agent requirements

Item	Requirement
CylanceOPTICS	• CylanceOPTICS version 2.3.2020 or later is required to configure communication through a proxy server only. • CylanceOPTICS version 2.4.2100 or later is required to enable Configurable Sensors in a device policy. • For desktops and laptops, Configurable Sensors requires Windows 10 or later. • For servers, Configurable Sensors requires Windows Server 2016 or later. **Note:** See Configurable Sensors for recommendations and details for using this feature. • CylanceOPTICS version 2.5.1100 or later is required for the Linux agent.
CylancePROTECT	• CylancePROTECT version 1400 or later • CylancePROTECT version 1468 or later required for Custom Endpoint Notifications • CylancePROTECT version 1560 or later required for the CylanceOPTICS Linux agent

Operating system requirements

For information about the operating systems that Optics 2.5.x supports, see the Cylance Endpoint Security compatibility matrix. To view support timelines for all BlackBerry products, see the BlackBerry Software Lifecycle Overview.

The following table lists the supported operating systems that have additional requirements or considerations. Note that this table is not a comprehensive list of supported operating systems. If an operating system is not listed in the table, it means that there are no additional requirements or considerations.

OS	Requirements or considerations
Windows 8.1 Windows 7 SP1	See this Microsoft article for additional dependencies for .NetCore support.
macOS Catalina (10.15) macOS Mojave (10.14)	Enable full disk access. For more information, see KB 66427.

OS	Requirements or considerations
RHEL/CentOS 8.x RHEL/CentOS 7.x Amazon Linux 2 Ubuntu 18.04	• kernel-headers and kernel-devel are required. The version depends on the kernel installed. This is handled by the package manager during installation. • One of the following Linux sensor suites is required: eBPF, Netlink (with multicast Netlink socket support 3.16 or later, or audit daemon uninstalled), or Auditdsp (with the auditd and auditdsp plugins enabled to start on boot). eBPF is recommended for the best performance with the Optics agent. If eBPF is not available, the agent tries to use Netlink for the next best level of performance. If Netlink is not available, the agent tries to use Auditdsp. The available sensor suites vary depending on the version of your OS. • Firewalld must be enabled to support the lockdown device feature. Firewalld is available by default with RHEL/CentOS and must be installed manually for Ubuntu and Amazon Linux. • For Amazon Linux 2 and RHEL/CentOS 8.x, ncurses-compat-libs is required.

Hardware requirements

Item	Requirements
CPU	Intel Core i5 processor or higher (or equivalent) is recommended 4 threads (2 cores + hyper-threading) or 4 cores
Memory	4GB
Available disk space	At least 1GB recommended CylanceOPTICS data stored locally can be over 100MB per day for business systems

Virtual machines

CylanceOPTICS is very resource intensive, and has a very specific set of Minimum Requirements to ensure functionality without negatively impacting performance. BlackBerry Engineering is in the process of delivering these Minimum VDI System Requirements to the support team. Until this is complete, support for CylanceOPTICS on VDI is Best Effort.

Workarounds

When using CylanceOPTICS on a virtual machine, use the following suggestions when attempting to resolve issues.

- Disable the WMI enhance introspection sensor. This can reduce the number of events being recorded.
- Try installing the latest version of the CylanceOPTICS agent.

Additional requirements

Item	Description
.NET Framework	Version 4.5 SP1 or higher Windows only
kernel-headers and kernel-devel	Version depends on the kernel installed Linux only
Internet connection	To register the product
Local administrator rights	To install the product

Network

CylanceOPTICS communicates over secure websockets (WSS) and must be able to establish this connection directly. For organizations that manage network traffic, like using a proxy, there are some Cylance hosts that the agent must be allowed to communicate with to properly display data in the Console.

Note: See the CylancePROTECT Administrator Guide for hosts specific for CylancePROTECT communications.

For CylanceOPTICS, allow the following domains (based on your region):

Region	Domains
Asia-Pacific Northwest	• cement-apne1.cylance.com • cylance-optics-files-apne1.s3.amazonaws.com • opticspolicy-apne1.cylance.com • content-apne1.cylance.com
Asia-Pacific Southeast	• cement-apse2.cylance.com • cylance-optics-files-apse2.s3.amazonaws.com • opticspolicy-au.cylance.com • content-apse2.cylance.com
Europe Central	• cement-euc1.cylance.com • cylance-optics-files-euc1.s3.amazonaws.com • opticspolicy-euc1.cylance.com • content-euc1.cylance.com
North America	• cement.cylance.com • cylance-optics-files-use1.s3.amazonaws.com • opticspolicy.cylance.com • content.cylance.com

Region	Domains
South America	• cement-sae1.cylance.com • cylance-optics-files-sae1.s3.amazonaws.com • opticspolicy-sae1.cylance.com • content-sae1.cylance.com

CylanceOPTICS Domain Descriptions

The following descriptions apply to all regions.

Domain	Description
cement.cylance.com	Detections, InstaQuery, Focus View, Refract Packages, and Refract Playbooks.
cylance-optics-files-use1.s3.amazonaws.com	InstaQuery results
opticspolicy.cylance.com	Download CylanceOPTICS policy settings
content.cylance.com	Download refract packages

Firewall

No on-premises software is required to manage endpoints. Agents are managed by and report to the console. Port 443 (HTTPS) is used for communication and must be open on the firewall in order for the agents to communicate with the console. The console is hosted by Amazon Web Services (AWS) and doesn't have any fixed IP addresses. Alternatively, you can allow HTTPS traffic to *.cylance.com.

Note: For the `cylance-optics-files-use1.s3.amazonaws.com` host (or similar host for other regions), it is recommended to allow that specific host. It is not recommended to allow `*.amazonaws.com` because it is not specific to the CylanceOPTICS host and can open up your network to other hosts.

Proxy

CylanceOPTICS is proxy aware and will query the .NET framework to see if a proxy is available. CylanceOPTICS will use the proxy settings and attempt to communicate; first as the Local System, then as the currently logged in user. There is also a registry edit (see the CylancePROTECT Administrator Guide) that configures the proxy settings for the CylancePROTECT Agent. These configuration settings will be used by CylanceOPTICS as well. This method requires that the proxy accept unauthorized requests out. If authentication is required, then this registry setting cannot be implemented.

Proxy support for CylanceOPTICS is configured through a registry entry, using the same process as configuring proxy support for CylancePROTECT. When a proxy is configured, CylanceOPTICS will use the IP address and port in the registry entry for all outbound communication to BlackBerry servers.

Access the Registry

1. In the Registry Editor, navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop

2. Create a new String Value (REG_SZ):
    a) Value Name = ProxyServer
    b) Value Data = proxy settings (For example, http://123.45.67.89:8080)

    In authenticated environments, CylanceOPTICS follows the same procedure as CylancePROTECT and attempts to use the credentials of the currently logged in user to communicate out to the Internet. If an authenticated proxy server is configured and a user is not logged onto the device, CylanceOPTICS cannot authenticate to the proxy and cannot communicate with the Console.

Disable Proxy Bypass

CylanceOPTICS is designed to maintain a connection to the Cylance cloud services. If a proxy server is configured and the Agent cannot communicate with the Cylance cloud services, the CylanceOPTICS Agent will attempt a direct connection to the cloud, bypassing the proxy server configuration. This can cause problems in organizations that want the Agent to only communicate through the proxy server. Starting with CylanceOPTICS version 2.3.2020, this proxy bypass feature can be disabled. This must be done before CylanceOPTICS is installed.

The DisableProxyBypass is only supported on Windows systems.

- Create a registry string value (REG_SZ) located at HKLM\SOFTWARE\Cylance\Optics\, with a Value Name set to DisableProxyBypass and the Value Data set to True.
- If this key is present, the CylanceOPTICS Agent will always attempt to establish a connection through the configured proxy server.

Windows API and Signed Files

When CylanceOPTICS creates a detection event that involves a signed file as one of the Artifacts, it will use a command from the Windows API to validate the signature/certificate. This command will generate traffic to an Online Certificate Status Protocol (OCSP) server with the validation request. The address of the server is determined by Windows, so the address may be different for different environments.

If your proxy is showing attempts to send external traffic to unauthorized addresses and you have a signed file as part of a CylanceOPTICS Detection Event, then check if the unauthorized address belongs to an OCSP server. If it is an OCSP server, users should update their proxy settings or allow communication with the OCSP server.

Download CylanceOPTICS from the Application page

Before installing CylanceOPTICS, you must download the install file.

1. Select **Settings > Application**.
2. Download the CylanceOPTICS installer.
    - **For Windows**, only the EXE file is available. For information about the PROTECT + OPTICS installation, see the CylancePROTECT Admin Guide.
    - **For macOS**, it is recommended to use the PKG file to install the Agent. The DMG file is simply a disk image of the PKG file, and is available for scenarios where a disk image must be mounted for installation.
    - **For Linux**, you can also download the agent UI, which is a separate file.

      Note: The agent UI is not available for Amazon Linux.

After you finish:

For installation information for each OS, review the following sections:

- Windows Installation
- macOS Installation
- Linux Installation

Note: If the Agent installer is not available or displays an error page, make sure the Zone-Based Updating is set to Do Not Update. In the Console, go to **Settings > Update** to change the setting to **Do Not Update**.

Windows Installation

Note: CylancePROTECT Agent 1400 or higher must be installed on the endpoint before you install CylanceOPTICS for Windows.

1. On the endpoint, double-click **CylanceOPTICSSetup.exe**. CylanceOPTICS can also be deployed using a group policy or other software management system.
2. Click **Install**.
3. Click **Close** when installation is complete. A system restart is not required (in rare cases, when Windows performs updates as part of the installation, a system restart is required). To verify the CylanceOPTICS installation, right-click the Agent icon in the system tray, then select About. The information includes the CylancePROTECT version and the CylanceOPTICS version.

Directory Locations - Windows

The following are the default installation locations on the Windows operating system.

- **Install directory**: C:\Program Files\Cylance\Optics
- **Data directory**: C:\ProgramData\Cylance\Optics
- **Log File Directory**: C:\ProgramData\Cylance\Optics\Log

Note: CylanceOPTICS retains a maximum of 10 log files, with a maximum size of 100MB per log file. The total number of days collected in the log files depends on the amount of data collected.

Windows Services

- **CyOptics** - The user-mode service that is the CylanceOPTICS product
  - **Display Name**: Cylance Optics
  - **Service Name**: CyOptics
  - **Path**: C:\Program Files\Cylance\Optics\CyOptics.exe
- **CyOpticsDrv** - The driver service that supports CyOpticsDrv.sys
  - **Display Name**: CyOpticsDrv

Windows Command Line Options

CylanceOPTICS Windows installation supports command-line options, including the following:

- **INSTALLFOLDER=** Allows users to define where CylanceOPTICS is installed on the endpoint

  For example, CylanceOPTICSSetup.exe INSTALLFOLDER=C:\Apps\Cylance\
- **OPTICSROOTDATAFOLDER=** Allows users to define where CylanceOPTICS stores the local database, configuration, and log files

  For example, CylanceOPTICSSetup.exe OPTICSROOTDATAFOLDER=C:\Storage\Cylance\
- Use **-q** or **-quiet** to perform a quiet installation, without any user intervention.
- Use **-s** or **-slient** to perform a silent installation, without any user intervention.
- Using **-q** or **-s** accomplishes the same thing.
- Use **-l**, **log** to capture log files during installation. For example, CylanceOPTICSSetup.exe -l c:\temp\install.log

- Use **-uninstall** to uninstall the product.

macOS Installation

Note: CylancePROTECT Agent 1480 or later must be installed on the endpoint before you install CylanceOPTICS for macOS.

1. On the endpoint, double-click the CylanceOPTICS installation package. If you use the DMG, you must open the DMG, then double-click the PKG.
2. Click **Continue**.
3. Click **Install**. A password might be required.
4. Click **Close** when the installation is complete. To verify the CylanceOPTICS installation, right-click the agent icon in the system tray, then select About. The information includes the CylancePROTECT version and the CylanceOPTICS version.

Directory Locations - macOS

The following are the default installation locations on the macOS operating system.

- **Install directory**: /Application/Cylance
- **Data directory**: /Library/Application Support/Cylance/Optics
- **Log File directory**: /Library/Application Support/Cylance/Optics/Log

Note: CylanceOPTICS retains a maximum of 10 log files, with a maximum size of 100MB per log file. The total number of days collected in the log files depends on the amount of data collected.

macOS Secure Kernel Extension Loading

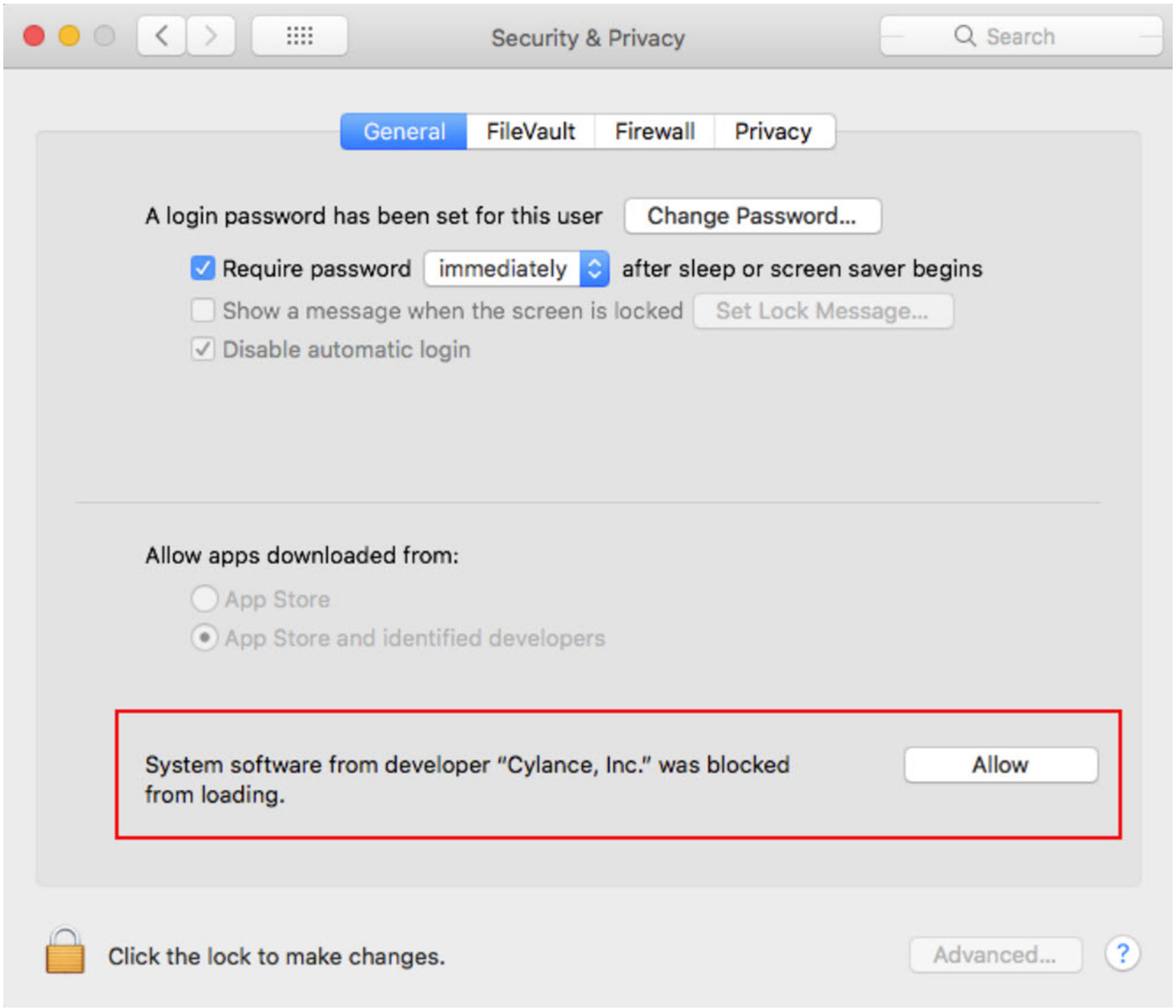
Starting with macOS High Sierra (10.13), an Apple security feature requires users to approve new third-party kernel extensions. If an unapproved extension tries to load, the extension is blocked and macOS displays an alert. Once approved by the user, the extension will load without any issues. This Apple feature is also called Gatekeeper.

Until the extension is approved, the Cylance shield displays a red dot. Clicking on the shield icon and selecting Show Details displays a message stating "Driver Failed to Connect. Device Not Protected."

For more information, including Enterprise deployments, see the macOS High Sierra Secure Kernel Extension Loading knowledge base article.

Note: This affects new CylanceOPTICS installations on macOS High Sierra or later. This will not affect CylanceOPTICS installed on macOS endpoints that are then upgraded to macOS High Sierra or later.

1. In the System Extension Blocked message, click **Open Security Preferences**. Or go to **System Preferences > Security & Privacy**.
2. Click **Allow**.



A login password has been set for this user

☑ Require password immediately after sleep or screen saver begins

□ Show a message when the screen is locked

☑ Disable automatic login

Allow apps downloaded from:

○ App Store

● App Store and identified developers

System software from developer “Cylance, Inc.” was blocked from loading.

Click the lock to make changes.

macOS Command Line Options

- **Install** : sudo installer -pkg CylanceOPTICS.pkg -target /
- **Install (Verbose, Troubleshooting)**: sudo installer -verboseR -dumplog -pkg CylanceOPTICS.pkg -target /
- **Uninstall**: sudo /Applications/Cylance/Optics/Uninstall\ CylanceOPTICS.app/Contents/MacOS/Uninstall\ CylanceOPTICS
- **Uninstall (No UI)**: sudo /Applications/Cylance/Optics/Uninstall\ CylanceOPTICS.app/Contents/MacOS/Uninstall\ CylanceOPTICS -noui
- **Start Service**: sudo launchctl load /Library/LaunchDaemons/com.cylance.cyoptics_service.plist
- **Stop Service**: sudo launchctl unload /Library/LaunchDaemons/com.cylance.cyoptics_service.plist

Note:

- A system reboot might be required after running the command.
- For macOS Catalina, when you install the CylanceOPTICS Agent using Terminal, a DYLD warning might display. This warning does not impact the installation. This warning is generated by the operating system, not by the CylanceOPTICS installer.

Linux Installation

Note:

- CylancePROTECT Agent 1560 or later must be installed on the endpoint before you install CylanceOPTICS for Linux.
- The Linux distro kernel must be supported by the CylancePROTECT agent.
- Kernel-headers and kernel-devel (version depends on kernel installed - this should be handled by the package manager on install).
- libelf (ELF library - this should be handled by the package manager on install).
- Firewalld must be enabled. This is required for Lockdown Device. firewalld should be available by default with RHEL/CentOS. firewalld must be installed manually for Ubuntu and Amazon Linux.

  Note: Lockdown Device is not supported on SUSE 12 (SLES 12).
- A reboot may be required after installing the CylanceOPTICS Linux Agent if the kernel is older or if the system has not been rebooted in a while.
- Trying to upgrade the CylanceOPTICS Linux agent from any version of 2.x to a newer version will fail if Security-Enhanced Linux (SELinux) is enabled. **Workaround:** Disable SELinux before upgrading Optics, then enable SELinux after the upgrade is complete.

Install RHEL/CentOS, SUSE, or Amazon Linux 2

Before you begin: Make sure CylancePROTECT is installed on the endpoint and is communicating with the Cylance Console.

1. Download the CylanceOPTICS Linux Agent RPM installation file for RHEL/CentOS, SUSE, or Amazon Linux 2.
2. Open the Terminal, navigate to the Downloads folder, then run `yum install CylanceOPTICS-version.rpm.`

   Note: Replace version with the version number included with the RPM file. Example: `CylanceOPTICS-2.5.1100.rpm.`
3. Close the Terminal when installation is complete.

Install Ubuntu

1. Make sure CylancePROTECT is installed on the endpoint and is communicating with the Cylance Console.
2. Download the CylanceOPTICS Linux Agent DEB installation file for Ubuntu.
3. Open the Terminal, navigate to the Downloads folder, then run `dpkg -i cylance-optics_version-release_amd64.deb.`

   Note: Replace version with the version number included with the DEB file. Example: `cylance-optics_2.5.1100.8444-release_amd64.deb.`
4. Close the Terminal when installation is complete.

Software Requirements - Linux

The CylanceOPTICS Linux Agent requires: kernel-headers and kernel-devel.

Note: The kernel-headers and kernel-devel versions should be handled by the package manager. However, a reboot may be required after installing the CylanceOPTICS Linux Agent if the kernel is older or if the system has not been rebooted in a while.

Directory Locations - Linux

The following are the default installation locations on the Linux operating system.

- **Install Directory**: /opt/cylance/optics
- **Log Directory**: /opt/cylance/optics/Log

Note: CylanceOPTICS retains a maximum of 10 log files, with a maximum size of 100MB per log file. The total number of days collected in the log files depends on the amount of data collected.

Stop or Start the Linux Service

Use the following commands to start or stop the CylanceOPTICS Service.

RHEL/CentOS 7.6, RHEL/CentOS 7.7, Amazon Linux 2, or Ubuntu 18.04

```
systemctl start cyoptics.service
```

```
systemctl stop cyoptics.service
```

Things to Know About the Linux Agent

Kernel Header and Develop Package

If the kernel-header and kernel-devel packages do not match the kernel, using yum update kernel and restarting the system should fix the issue.

If a system restart is not possible, try:

- **For RHEL/CentOS or Amazon Linux 2**: `yum install kernel-headers-`uname -r` kernel-devel-`uname -r``
- **For Ubuntu**: `sudo apt-get install linux-headers -$(uname -r)`

Check the Kernel Package

Use `uname -r` to check the currently running kernel.

Data in Debug Logs

When debug logging is enabled, CylanceOPTICS will record messages like "Corroborator found a match for PID 2434 running at 1/28/2020 12:00:00 PM." This is not recording a bug or other issue, it is the product confirming a match for what it is looking for. This is expected behavior.

Uninstalling CylanceOPTICS

Uninstalling CylanceOPTICS also removes all CylanceOPTICS focus data and log files from the device. To uninstall CylancePROTECT, see the CylancePROTECT Administrator Guide.

Note:

- Uninstalling CylanceOPTICS will result in a loss of all CylanceOPTICS data on that device, including CylanceOPTICS log files. If you are troubleshooting, you should save the CylanceOPTICS log files to a different location prior to uninstalling the product.
- CylanceOPTICS must be uninstalled before uninstalling CylancePROTECT.

Uninstall Windows using Add/Remove Programs

This is the recommended method for most users.

1. Log in to the endpoint you want to remove CylanceOPTICS from.
2. Open **Programs and Features**. For example, click **Start > Control Panel > Uninstall a program**.
3. Select **CylanceOptics > Uninstall**.
4. When the uninstall process completes, click **Close**.

Uninstall Windows using the Command Line

Uninstall the Windows Agent from the command-line for a non-interactive uninstallation.

1. The user uninstalling CylanceOPTICS must take ownership of the files and directories owned by the local system. If done by an administrator, it is required that Windows policy allows for administrators to take ownership of files and directories.
2. To check if administrators have the required permissions, do the following:
   a) Launch secpol.msc.
   b) Under **Local Policies**, select **User Rights Assignment**.
   c) Scroll to the bottom of the list and make sure **Take ownership of files or other objects** is set to **Administrators**.
3. The following command is an example for a non-interactive uninstall. It is best not to navigate to the CylanceOPTICS program directory because that directory needs to be deleted. By including the absolute path in the command, it can be run from any directory.

   Example: C:\Program Files\Cylance\Optics\CyOpticsUninstaller.exe --use_cli -t v20

Uninstall macOS

1. Log in to the endpoint for which you want to remove CylanceOPTICS.
2. Open **Finder**, then select **Applications**.
3. Expand **Cylance**, expand **Optics**, then double-click **Uninstall CylanceOPTICS**.
4. Click **Yes**.
5. Type the user password.
6. Click **OK**.

Uninstall Linux

Use the following command to uninstall the Linux Agent, based on the operating system.

For RHEL/CentOS or Amazon Linux 2:

```
rpm -e CylanceOPTICS
```

For Ubuntu:

```
dpkg -P cylance-optics
```

Upgrading to v2.5

It is recommended that users take a phased rollout strategy for CylanceOPTICS. The best practice for this is to set the production zone for zone-based updating (located on the **Settings > Update** page in the Console) to **Do Not Update**.

To update endpoints in the test or pilot zones, set the CylanceOPTICS version to the latest version or select **Auto-Update**, which will automatically push out updates to all endpoints in a zone as the endpoints become available (online).

Note: Trying to upgrade the CylanceOPTICS Linux agent from any version of 2.x to a newer version will fail if Security-Enhanced Linux (SELinux) is enabled. **Workaround:** Disable SELinux before upgrading Optics, then enable SELinux after the upgrade is complete.

Edit a Policy

After CylanceOPTICS has been enabled in a policy, the agent starts collecting events and storing that data on the device. The default policy allocates up to 1000 MB of storage space on each device running CylanceOPTICS. When the storage space is exhausted, CylanceOPTICS will purge the oldest data and overwrite it with the most current events.

The amount of storage space allowed can be configured in a policy. The setting goes from 500 MB to 1000 MB.

1. In the console, select **Settings > Device Policy**.
2. Create a new policy or edit an existing policy.
3. Select **CylanceOptics Settings**.
4. Select the **CylanceOptics** checkbox to enable CylanceOPTICS.
5. Select any of the following features:

   - **Threats - Auto Upload** automatically uploads threat-related focus data from the agent to the console. If this is not enabled, then an administrator must click **Request Focus Data** in the console to retrieve the data.
   - **Memory Protection - Auto Upload** automatically uploads memory-related focus data from the agent to the console. If this is not enabled, then an administrator must click **Request Focus Data** in the console to retrieve the data.
   - **Configurable Sensors** allows the CylanceOPTICS agent to record additional events (beyond the standard process, file, network, registry, and thread events).

     Note: Enabling configuration sensors may increase the amount of data being stored. This would reduce data retention in the local CylanceOPTICS database.
   - **Set the maximum storage reserved on the device for use by CylanceOPTICS** sets the maximum amount of storage CylanceOPTICS can use on the device. The capacity range is from 500 MB to 1000 MB.
   - **Enable CylanceOptics Desktop Notifications** enabled desktop notifications on the device.
   - **Detection Settings** allows selecting a detection set for the policy.
6. Click **Save**.

   Note: Do not use Application Control when using CylanceOPTICS. Application Control is a CylancePROTECT feature designed for fixed function devices that are not changed after setup (example: point-of-sales machines). When Application Control is enabled, CylanceOPTICS will not function properly due to the restrictive nature of Application Control. For more information about Application Control, see the CylancePROTECT Administrator Guide.

Configurable Sensor Descriptions

Note: See Configurable Sensors for recommendations and details for using this feature.

Configurable Sensor	Description
Advanced Scripting Visibility	Ability for the CylanceOPTICS Agent to record commands, arguments, scripts, and content from JScript, Powershell (console and integrated scripting environment), VBScript, and VBA macro script execution
Advanced WMI Visibility	Ability for the CylanceOPTICS Agent to record additional Windows Management Instrumentation (WMI) attributes and parameters

Configurable Sensor	Description
DNS Visibility	Ability for the CylanceOPTICS Agent to record DNS requests, responses, and associated data fields such as Domain Name, Resolved Addresses, and Record Type made by processes
Enhanced File Read Visibility	Ability for the CylanceOPTICS Agent to monitor file reads within an identified set of directories **Note:** Requires CylanceOPTICS agent version 2.5.3000.
Enhanced Portable Executable Parsing	Ability for the CylanceOPTICS Agent to record data fields associated with Portable Executable (PE) files such as File version, Import functions, and Packer types
Enhanced Process and Hooking Visibility	Ability for the CylanceOPTICS Agent to record process information from the Win32 API and Kernel Audit messages to detect forms of process hooking and injection
Private Network Address Visibility	Ability for the CylanceOPTICS Agent to record network connections within the RFC 1918 and RFC 4193 address spaces
Windows Advanced Audit Visibility	Ability for the CylanceOPTICS Agent to monitor additional Windows event types and categories **Note:** Requires CylanceOPTICS agent version 2.5.3000.
Windows Event Log Visibility	Ability for the CylanceOPTICS Agent to record Windows Security Events and their associated attributes

Things to Know about the Optics Policy

Starting with version 2.3.2021, CylanceOPTICS will not automatically start collecting data after it is installed. In the Cylance Console, CylanceOPTICS is not automatically enabled in a policy. Administrators must enable CylanceOPTICS for new policies.

- The CylanceOPTICS ON / OFF checkbox (under CylanceOPTICS Settings) only controls data collection.
- If CylanceOPTICS is OFF (checkbox is unchecked) and auto upload for focus data (threats or memory protection) is still enabled, auto upload of focus data will continue. Auto upload must be disabled (checkboxes are unchecked) for each category in order to stop automatically uploading focus data.

Devices

The CylanceOPTICS devices page lists endpoints with the agent installed.

Item	Description
Device	The name of the device
Status	Shows if the device is online or offline
CylanceOPTICS version	Showed the version of CylanceOPTICS installed on the device
IP address	The IP address for the device
Zones	The zone the device is assigned to
Details	The View link goes to the Device Details page for the device
Actions	Shows lockdown details for the device • **Lockdown Status** shows if the device is locked or unlocked • **Est. Time Remaining** shows the amount of time remaining before the device is automatically unlocked • **Lockdown Device** allows you to lock a device; the device must be online • **Show Unlock Key** shows the key needed to manually unlock the device
Filter	Enter a value to use as a filter on all columns
Show Download History	Shows files downloaded from a device and the user who made the request

Device Drawer

The CylanceOPTICS Device Drawer provides some details about the device. To view the Device Drawer, click on the device name link. The Device Drawer appears as a slide-out information window. The Device Drawer contains the following details about the endpoint:

Note: The CylanceOPTICS Devices page does not display devices that have been offline for more than 90 days.

- **CylanceOPTICS Version** shows the CylanceOPTICS version installed on the endpoint.
- **Device Name** shows the name of the endpoint.
- **Hostname** shows the hostname for the endpoint.
- **IP Address** shows all IP addresses identified for the endpoint.
- **Select Action** shows which actions can be performed on the endpoint from the Device Drawer.
  - **Lockdown** allows administrators to lockdown the endpoint.
  - **Package Deploy** allows administrators to deploy a CylanceOPTICS package to the endpoint.
- **Status** shows if the endpoint is online or offline.
- **Zones** shows all zones assigned to the endpoint.

Export device list

Export a .csv file containing details about your CylanceOPTICS devices.

1. In the console, select **CylanceOPTICS**.
2. Select **Devices**.
3. Click **Export**.

Device export descriptions

The exported Devices .csv file contains the following information.

Item	Description
Device	Name of the device
Status	Status of the device is Online or Offline
CylanceOPTICS Version	Version of the CylanceOPTICS agent installed on the device
IP Address	IP address used by the device
Zones	Zones the device is associated with

Device details page

Optics information is integrated with the device details page in the console.

Item	Description
CylanceOPTICS status	• Online • Locked down • When a device is locked down, a tooltip appears next to the status. Hovering over the tooltip displays the estimated time remaining for the lockdown and the unlock key.
Device actions	Optics actions are available on the device actions dropdown menu on the device details page. Actions include: • Lockdown • Package deploy • Remote response

Role Management

Console administrators can create custom roles (Role Based Access Control or RBAC) or use a predefined role to manage users access to features.

Predefined roles

- Administrators have global permissions and can see all threats, devices, and zones.
- Users and Zone Managers have access and only to the Zone that they are assigned to. This applies to devices assigned to the Zone, threats found on those devices, and information on the dashboard.
- The CylanceOPTICS feature does not display for Read-only users.

Custom roles

You can use custom roles to customize access to Console features and assign users to this custom role. Enabling the CylanceOPTICS page access allows users to interact with all the CylanceOPTICS tabs. This includes features like InstaQuery, Focus Data, Lockdown, and Remote Response.

Note:

- Users cannot view the Console Devices page, just the CylanceOPTICS Devices page. To view the Console Devices page requires the Devices Custom Role permission be enabled.
- For more information about Role Management, read the CylancePROTECT Administrator Guide.

Using InstaQuery

InstaQuery (IQ) is the CylanceOPTICS search feature designed to help you discover Indicators of Compromise (IOC) and determine its prevalence on our devices. InstaQuery searches specifically within the realm of artifacts, not events. This means InstaQuery will not tell you about how or when an artifact (like a file or process) was used but instead tell you whether an artifact has ever been observed in a forensically interesting way. Once deployed, CylanceOPTICS starts collecting all new artifacts and stores them in the CylanceOPTICS database on the endpoint. InstaQuery then retrieves data from these databases, returning the results and storing them in the cloud and making those results available through the Cylance Console.

InstaQuery is a fast, efficient way to interrogate a set of devices about the observation of a particular type of forensic artifact. IQ answers the questions: "Does this artifact exist?" and "How common or uncommon is this?"

Note: Console administrators can see all InstaQuery results in their organization. Zone managers and users can only see the query results they have created.

InstaQuery Capabilities Descriptions

Artifacts and Facets

InstaQuery has the following capabilities on what can be searched:

Capability	Description
Examines artifacts, not events	InstaQuery results will tell you if something has been observed, not what it did or how it was used.
CylanceOPTICS responds to InstaQuery queries with data that is currently indexed	InstaQuery, for efficiency and from a forensic standpoint, answers queries with data that CylanceOPTICS has available and has deemed forensically interesting.
Searches against a single facet of a single class of artifacts	These can be searches for processes by command-line.

Specific Artifact Types and Their Limitations

InstaQuery can search against the following artifact types:

Artifact	Description
Network Connections	CylanceOPTICS currently exposes the ability to perform IQ queries against Destination IP addresses, both IPv4 and IPv6. See CylanceOPTICS Network Visibility for considerations about the types of network traffic that CylanceOPTICS is configured by default to ignore. In brief, CylanceOPTICS currently discards private, non-routable, multicast, link-local, and loopback network traffic.

Artifact	Description
Processes	All processes are currently indexed into the CylanceOPTICS database. There are some restrictions: • Command-lines are currently limited to 1KiB of data. • Process names are limited to 256 characters. • Process image file paths are limited to 512 characters. • Command-lines that are altered after the process has started are not currently monitored.
Files	• Files that are created, modified, or deleted can be queried via IQ. This is after CylanceOPTICS is installed. • CylanceOPTICS focuses on files that can be used for execution of content, and therefore focuses on executable files, Office documents, PDFs, etc. • File paths are limited to 512 characters.
Registry Keys	• Registry key paths are limited to 256 characters. • Registry value names are limited to 128 characters. See CylanceOPTICS Registry Introspection for considerations about the types of registry key activity that CylanceOPTICS is configured by default to ignore. In brief, CylanceOPTICS monitors only persistence points and file deletion points in the registry, which are areas typically harnessed by malware for surreptitious purposes.
IQ Results and Retention	InstaQuery limits both the search space, time, and retention. This is to maintain the performance of IQ queries. • Will display and retain up to 10,000 results for a single query. This is a design decision that emphasizes that IQ is a high-performance, lightweight query mechanism for finding anomalies or prevalence. • Results are only retained in the cloud for 30 days for a particular IQ query.

Start an InstaQuery

1. In the Console, select **CylanceOPTICS**. The InstaQuery tab displays.
2. To create a query, add the following:
   a) Type a search term. You can also select exact matching to restrict the search results.
   b) Select an artifact.
   c) Select a facet.
   d) Select a zone or zones. When you select zones, you can see the total number of endpoints in the zone and the number of endpoints online (for that zone). If a zone has no online endpoints, you cannot select it for an InstaQuery. With no online endpoints, the InstaQuery would return no results.

      Note: If all the online endpoints go offline before you run the query, the InstaQuery will return no results.
   e) Type a name for the query.
3. Optionally, you can add a description for the query.
4. Click **Submit Query**.

View InstaQuery Results and Previous Queries

Expand the previous queries section. This displays the original results of the query. This does not re-run the query.

1. In the Console, select **CylanceOPTICS**.
2. Expand the **Previous Queries** section.
3. Select an existing InstaQuery.

   Note: Data retention is 30 days for CylanceOPTICS data, including the InstaQuery results.

Global Quarantine

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

1. In the console, select **CylanceOPTICS**.
2. Select **InstaQuery**.
3. View a previous query.
4. From the InstaQuery Results page, click the **Actions** menu.
5. Select **Global Quarantine**, type in a reason for quarantining the file.
6. 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.

Download 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 administrations in the Cylance Console.

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

The file size limit for file retrieval is 50 MB.

Note: Data retention is 30 days for CylanceOPTICS data, including successful download requests.

1. In the Console, select **CylanceOPTICS**.
2. Select **InstaQuery**.
3. View a previous query.
4. From the InstaQuery Results page, click the **Actions** menu.
5. If this is the first time downloading the file, click **Request File Download**. The button changes to File Pending as the request is processed.
6. Click **Download File** when the file is ready. The Download File windows displays.
7. Click **Confirm Download**. The file is downloaded as a password protected, compressed file. The password is infected.

Export InstaQuery list

You can export a .csv file that contains details about the queries on your InstaQuery page.

1. In the console, select **CylanceOPTICS**.
2. Select **InstaQuery**.
3. Expand the previous queries.
4. Click **Export**.

InstaQuery export descriptions

The exported InstaQuery .csv file contains the following information.

Item	Description
Name	The name of the query
Description	The description of the query; this is entered by the user who created the query
Created On	The date and time the query was created
Artifact	Type of item the search is being conducted for
Facet	Artifact attribute the search is being conducted for
Term	Specific value the search is being conducted for
Zones	Zones included in the query

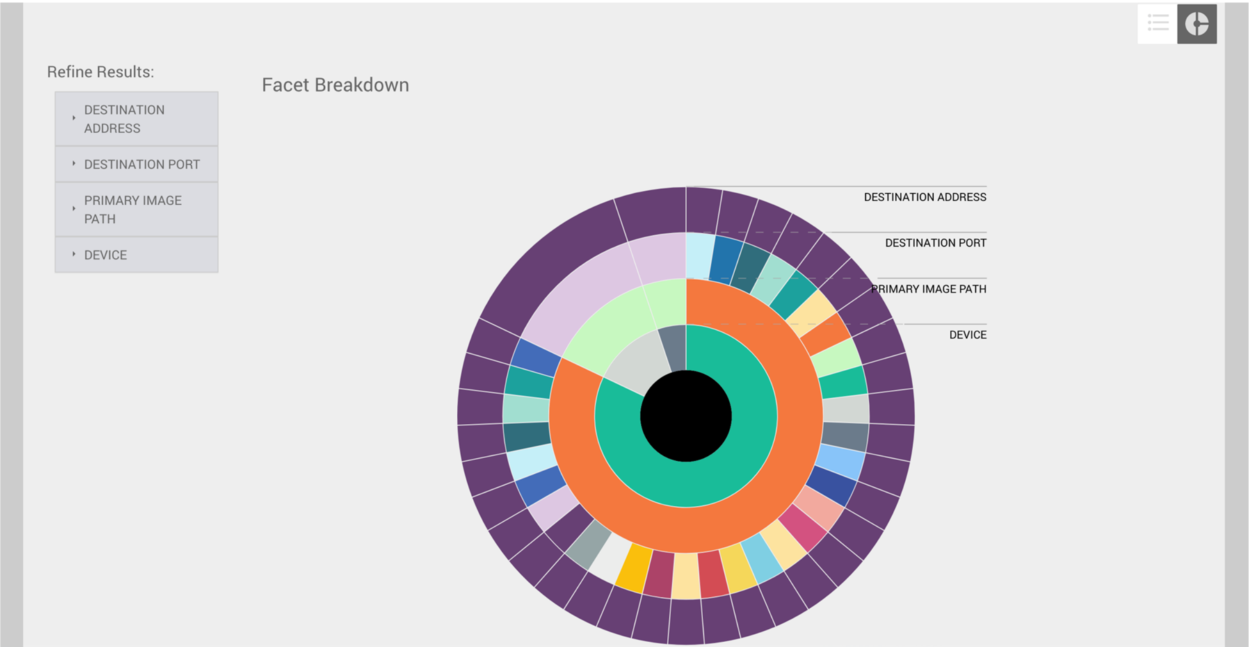
InstaQuery Facet Breakdown

The InstaQuery (IQ) Facet Breakdown provides a visual display of the different facets and allows a user to follow the relational path of the different facets identified.

Visualizing data in a sunburst model can be useful for finding suspicious activity in datasets that may be difficult to observe in other formats. For example, when hunting for suspicious network connections across an entire environment or multiple device zones, data patterns and anomalies may be difficult to quickly identify because of the sheer volume and complexity of data that needs to be analyzed. The following images show how a user can interact with the InstaQuery Facet Breakdown sunburst chart to quickly locate suspicious activity by visualizing and filtering complex technical data.

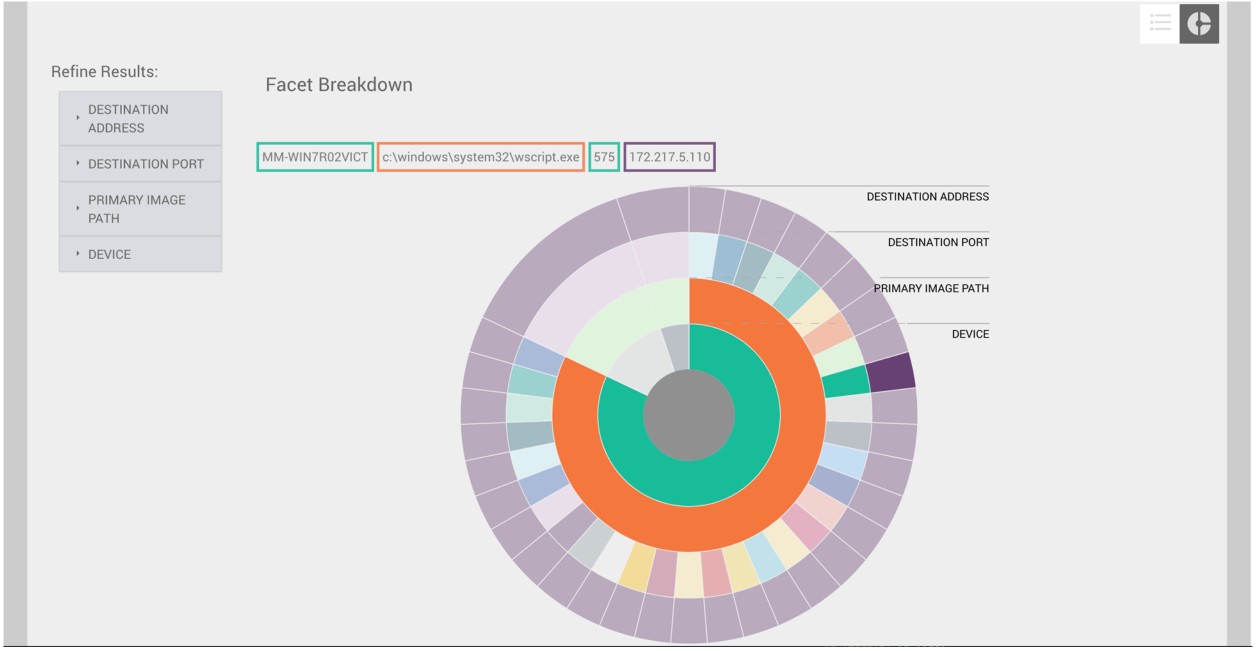
The images used for this example were generated by using an InstaQuery to search an entire CylanceOPTICS deployment for connections to a specific IP address. The results of this InstaQuery were automatically visualized into the sunburst diagram with the following facets: Device, Primary Image Path, Destination Port, and Destination Address.

Note: Data retention is 30 days for CylanceOPTICS data, including the InstaQuery results.



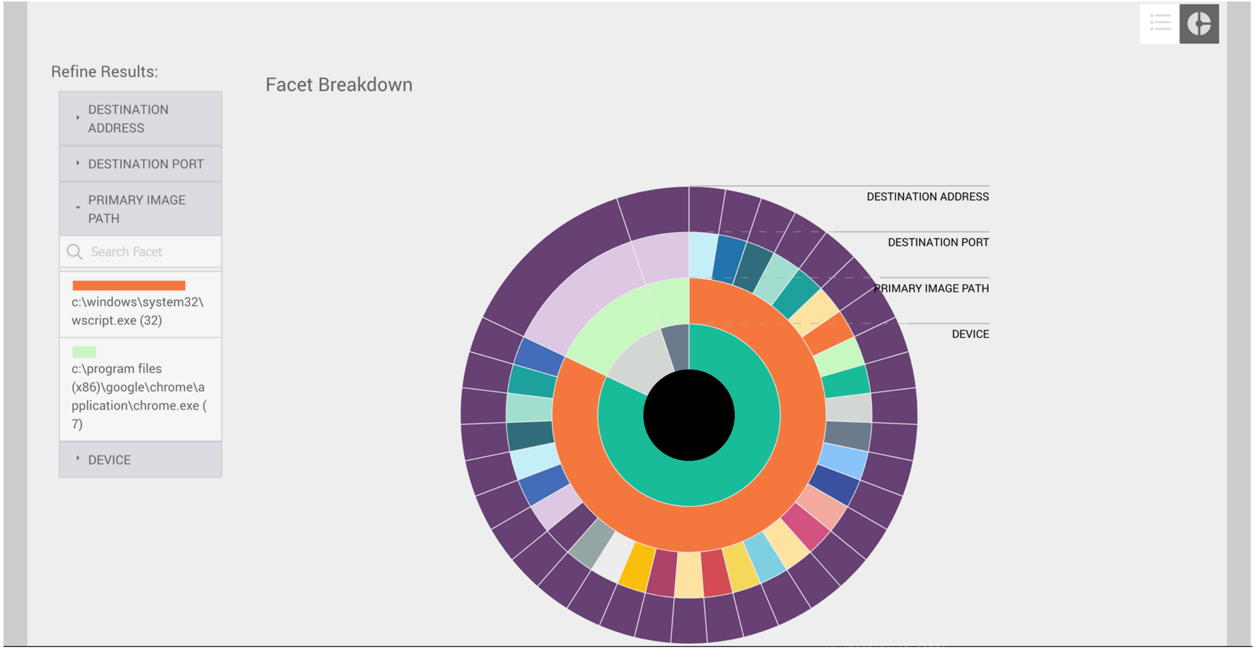
As a user begins to observe patterns in the sunburst chart, they can hover over any of the different facets to display their associated values. In the image below, the outermost facet is selected, allowing the user to observe the name of the device where the connection was recorded, the path to the file that initiated the network connection, the port number being used in the connection, and the IP address of the remote system.

As each relevant facet is hovered over, its associated parent facets are also highlighted to help the user draw a visual relationship between the data points. In this example, we can see that one device and one parent process were responsible for most connections to the IP address in question. We can also see that many different network ports were used to connect to this IP address from the associated host, something that differs from the other two host facets present in the sunburst.

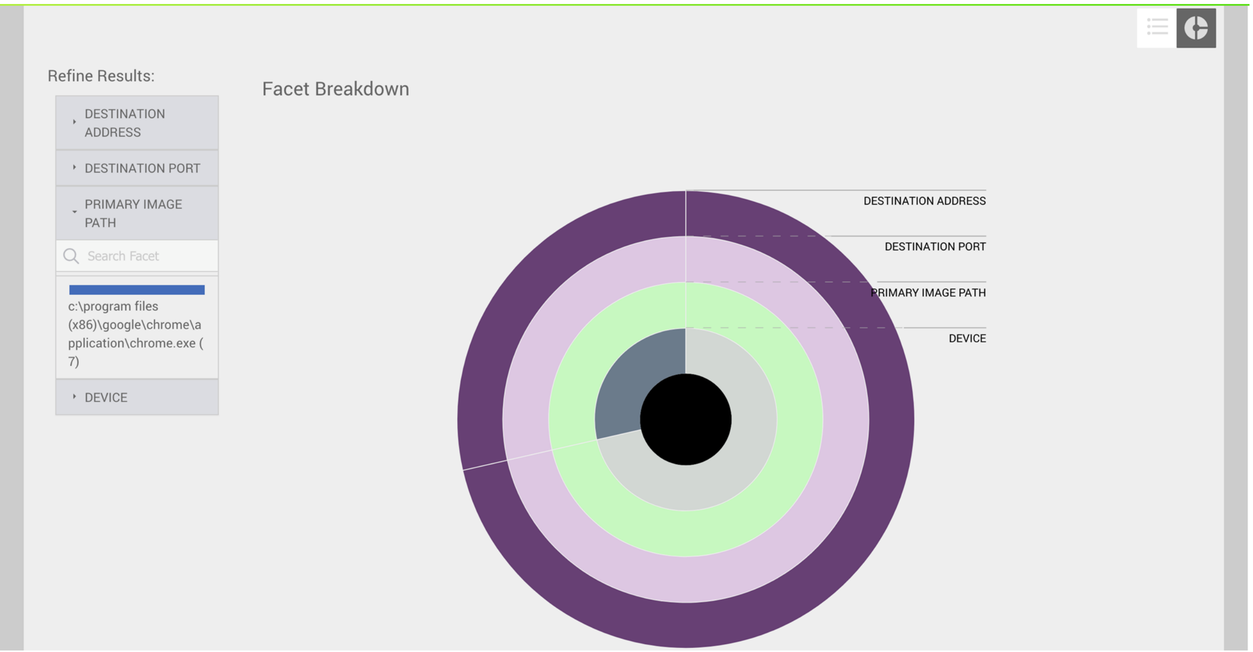


MM-WIN7R02VICT c:\windows\system32\wscript.exe 575 172.217.5.110

A similar result can be achieved by utilizing the Refine Results menus. Each of the Facet Menus contains the unique values and number of occurrences for each facet that is present in the sunburst chart. In the example below, a user can see that there were two processes responsible for connections to this IP address: Google Chrome and Wscript.



Clicking a facet value in the Refine Results menu will cause the sunburst chart to automatically filter to only display directly related facets. This is particularly useful for filtering out irrelevant or uninteresting data in large datasets to help create a more focused analysis environment.



InstaQuery Troubleshooting

If you encounter a situation where you are coming up against the limit to responded devices or the limit of the maximum number of results, consider the following.

Situation	Description
Is there a more specific way to ask the question?	For example, consider using specific matching, case-sensitive matching, or making the search term more specific.
Does the large number of results answer the question?	For example, if you are searching for the prevalence of a particular IoC, the high prevalence of it might indicate that the IoC is erroneous or might imply that the IoC is likely on other devices not shown in the result set.
Is there an inverse to the question you are asking?	

InstaQuery Results Descriptions

The following tables provide short descriptions for each InstaQuery result or facet.

InstaQuery Results Summary

InstaQuery Result	Description
Artifact	Type of item for which the search is being conducted
Date Create	Date the InstaQuery was created
Description	Description of the InstaQuery
Devices Queried	Total number of endpoints associated with the query
Devices Responded	Number of endpoints that responded to the query request
Devices with Results	Total number of endpoints that matched the query
Facet	Artifact attribute for which the search is being conducted
Name	Name of the InstaQuery
Term	Specific value for which the search is being conducted
Total Results	Total number of artifacts returned from the query
Zones	Zones and endpoints in the zones included in the query

InstaQuery Results - Artifact Type: DNS

Facet	Description
Question Address	The IP address to query.
Question Entropy	The randomness to query. "How random is this question?"
Question Name	The domain name to query. "Has mydomain.net been seen?"
Question Type	The record type to query.
Record Value	The domain name resolution to query. "Has a domain ever resolved to this?"
Response Address	The IP address to query.
Response Entropy	The randomness to query. "How random is this response?"
Response Type	The record type to query.

InstaQuery Results - Artifact Type: File

Facet	Description
Created	The date the file was created.
Device	The name of the endpoint upon which the file was found.
MD5	The MD5 hash for the file.
Owner	The name of the user that owns the file.
Path	The path to the file.
SHA256	The SHA256 hash for the file.

InstaQuery Results - Artifact Type: Powershell Trace

Facet	Description
Entropy	The randomness to query. "How random was the script text?"
Event ID	The Event ID to query. "Show me all matches for Event ID 4101."

Facet	Description
Is Content Truncated	Query whether or not the content is truncated.
Original Size	The original size of the script to query.
Payload	The text to query for in the payload. "Has a payload or module executed with this text in it?"
Script Block Text	The text to query for in the script block. "Has a script executed with this text in it?"

InstaQuery Results - Artifact Type: Process

Facet	Description
Command Line	The command used to initiate the process.
Device	The name of the endpoint upon which the process was found.
Image MD5	The MD5 hash for the file.
Image Path	The path to the process executable file.
Name	The name of the process.
Owner	The owner of the process.
State Date	The date and time the process was started.

InstaQuery Results - Artifact Type: Network Connection

Results displayed for the network connections are filtered if the connection is entirely localized to certain IP ranges, such as the following:

- Private
- Linklocal
- Non-routable
- Multi-cast
- Loopback

Facet	Description
Destination Address	The IP address to which the source is connecting. **Note:** All queries are run on destination IP addresses only.
Destination Port	The port number the source IP address is trying to use to connect to the destination.
Device	The name of the endpoint.

Facet	Description
Image Path	The path to the process executable file.
Process Name	The name of the process related to the Network Connection.

InstaQuery Results - Artifact Type: Registry

From the InstaQuery results page, a user can take further response actions under the Action row, as well as discard a query, which will remove it from the Previous Queries list.

Facet	Description
Device	The name of the endpoint.
File MD5	The MD5 hash for the file.
File Path	The file path to the extracted registry key, value, or value contents.
Is Persistence Point	CylanceOPTICS monitors persistence points in the registry.
Path	The path to the registry hive.
Value Name	The registry value.

InstaQuery Results - Artifact Type: Windows Events

Facet	Description
Class	The class ID to query. "Show me all Logon / Logoff events."
Event ID	The Event ID to query. "Show me all matches for Event ID 4624."
Provider ID	The security provider ID to query. "Show me all events from the Security / Audit provider."

InstaQuery Results - Artifact Type: WMI

Facet	Description
Checksum	The checksum to query.
Consumer Text	The text to query. "Has a WMI consumer text been created with this text in it?"
Entropy	The randomness to query. "How random was the consumer text?"

Facet	Description
Event ID	The Event ID to query. "Show me all matches for Event ID 5861."
Is Content Truncated	Query whether or not the content is truncated.
Name Space	The name space to query. "Has a payload or module executed with this text in it?"
Operation	The operation to query. "Has a WMI operation executed with this text in it?"
Original Size	The original size of the artifact to query.
Originating Machine Name	The machine name to query.

Focus Data

Focus data provides an information trail starting with the first event related to the 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. See below.

Note: Data retention is 30 days for CylanceOPTICS data, including focus data.

About Focus Data

- The time for CylanceOPTICS to return focus data 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 customers' 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
Artifact Type	Artifact from either the InstaQuery search or the CylancePROTECT event
Created Date	Date on which the focus view was requested
Descriptions	Facet value of the query, the name of the associated file from an exploit attempt, or the path for a threat
Devices	Name of the device associated with the focus view
Focus Data	Link to view the focus data

Administrators can see all focus views, while zone managers and users can only see focus views for devices in the zones to which they are assigned.

If a focus view has been requested for an artifact in an InstaQuery, the focus view can also be viewed from those query results.

Threats and Activities

In the console, the Focus View column is displayed on the Device Details page and will have a link to the CylanceOPTICS focus data. If auto-upload is not enabled in the device policy, then an administrator must click the Request Focus Data link to initiate retrieving the data. Depending on the amount of data, it could take several minutes before the focus data is available. When the focus data is ready, the link will change from Data Pending to View Focus Data.

After clicking the View Data link, the Focus Data page displays the timeline of events related to the threat.

Export Historical List View

The historical list view can be exported as a .csv file so data can be filtered using a spreadsheet program, like Microsoft Excel.

- On the Focus View page, click the **Table View** button (upper-right).
- Once in Table View, click the **Export Results** button.

Pivot Queries

In a focus view, you can create an InstaQuery for an artifact or facet in a focus view. Artifacts and facets that can have pivot queries run against them have a UI button, that when clicked, will present an action to create an InstaQuery.

When you click the **Create InstaQuery** button, an InstaQuery windows displays, with the artifact or facet properties already added to the query. Just add the device zones that should be queried and click the **Submit Query** button.

After you submit the query, the Pivot Queries panel (beneath the focus view) will be updated with the submitted pivot query data. You can navigate pivot query data the same way as an InstaQuery.

Pivot queries are linked with their associated focus views and will be available anytime a focus view is revisted.

Detections

The CylanceOPTICS Detections feature is powered by the Context Analysis Engine (CAE) - a highly performant and optimized engine that statefully analyzes and correlates events as they occur on an endpoint in near real time. The CAE stores its logic locally on the endpoint, allowing it to monitor and track malicious or suspicious activities on an endpoint even when no connection to Cylance's cloud services is available. This architecture also helps negate potential performance impacts; not requiring an active network connections to intelligently make decisions allows the CAE to track many instances of many logic paths in near real time.

To complement the capabilities of the CAE, CylanceOPTICS can take automated response actions against Artifacts of Interest (AOI) identified by the CAE. These Response Actions, again, are stored locally on the endpoint, allowing CylanceOPTICS to function as another layer of prevention in addition to CylancePROTECT, even when the endpoint does not have access to Cylance's cloud services.

A dashboard allows customers to quickly understand and view trends of events of interest that are occurring across their environment. From this dashboard, users can investigate or respond to these events in a meaningful manner without needing to leave Cylance's Console. The CAE can be easily configured to fit many environments by creating detection rule sets that can be applied to one or more device policies. To create a unified experience, the new Detections section of the Console was designed with integration into other CylanceOPTICS features in mind. As such, events and artifacts identified by the CAE can be extended upon by creating additional focus views, retrieving files of interest with the file retrieval features, or quarantining an endpoint on the network by issuing a Device Lockdown.

Note: CylanceOPTICS Context Analysis Engine and Response Actions require CylanceOPTICS 2.1.1000 or higher and CylancePROTECT 1400 or higher.

Detection Environment Overview

To assist users with setting up their CylanceOPTICS detections, the Detections page (**CylanceOPTICS > Detections**) displays the three configuration requirements:

- The number of devices with CylanceOPTICS version 2.1.1000 (or later) installed
- The number of Detection Rule Sets configured
- The number of Device Policies with a Detection Rule Set selected

A green box indicates the requirement has been met. Once all three configuration requirements are complete, the CylanceOPTICS Detections page will display a graph and a table with detection events.

Note: A default detection rule set is provided, so the Number of Configured Detection Sets should be a green box.

First Time Using Detection Rule Sets

The center box on the onboarding page displays the number of Detection Rule Sets that exist in the tenant. Detection Rule Sets are the central configuration point for the CAE that determine the Detection Rules, Automated Responses, and Endpoint Notifications that are applied to endpoints. Detection Rule Sets are ultimately applied to endpoints on a Device Policy basis; that is, a user will select a Detection Rule Set to apply to a Device Policy. Endpoints will automatically receive the desired Detection Rule Set when the policy is applied.

CylanceOPTICS includes a default Detection Rule Set that has the following attributes:

- All official rules provided by Cylance are enabled
- All automated actions are disabled
- All endpoint notifications are disabled

The configuration is designed to act as an Alert-only mode for testing and initial deployment purposes. Users will gain an understanding of areas of their environment that may trigger false-positives, so that automated response actions can be tuned accordingly.

Detection Tab

The Detection tab provides users with a view into alerts triggered by endpoints configured with the CAE. From this dashboard, users can see trends in events over varying time frames, the severity of different detections, and a summary view of each of the detections that has occurred. Filtering and sorting features present in the dashboard allow users to further drill into the data presented to further identify trends throughout the environment.

Each detection event contains an entire series of data that can be viewed by clicking the View button. The resulting Detection Details page displays a wealth of information about the detection, including the detection's name, severity, number of events, AOIs, and automated responses associated with the detection.

Detection Status Event

The detection event status allows you to track the progress when working to resolve the event.

- Change the status to know where in the workflow the detection is: New, In Progress, Follow Up, Reviewed, or Done.
- Select multiple detection events and change them to the same status.

Status	Description
Done	All work is complete for this detection event.
Follow Up	Work was done, but a follow up is required.
In Progress	Work is being done on the detection event.
New	No work has been done on the detection event.
Reviewed	The detection event has been reviewed.

Delete Detection Events

From the Detections tab, you can select one or more detection events and delete them.

1. In the console, click **CylanceOPTICS**.
2. On the **Detections** page, select one or more detection events in the table. Selecting one or more events causes the Select Action menu to display.
3. From the Select Action list, select **Delete Detection**.
4. Confirm the deletion.

Detection Details Page

The Detection Details page provides information about an event, allows you to lockdown the endpoint to stop it from communicating over your network, and provides details about AOI.

View Artifacts of Interest

AOI are events selected by the CAE as the most relevant to the detection. The goal is to provide administrators with important information instead of a long list of all events related to the detection.

1. In the console, click **CylanceOPTICS**.
2. On the Detections tab, click the **View** icon for the detection event. The Detection Details page displays.
3. Click the number of Total AOI. **Total AOI** is located at the top of the Detection Details page.
4. Select one of the artifacts from the list. The artifact details display at the bottom of the page.
5. With the artifact details displayed, you can click on any of the artifact names to view those details.
6. To request focus data for the artifact, click the **Actions** menu.
7. Click **Request Focus Data**.

Create a Detection Note

You can add a note about a detection in the Detection Details page. Use this to retain important information about the detection that is not in the details. This could be information uncovered while investigating the event, a solution used to resolve the event, or details about the status of the event. One note can be added to the detection details, up to 1,024 characters (including spaces).

1. In the console, click **CylanceOPTICS**.
2. Click on a detection event to view the Detection Details.
3. On the Detection Details page, click **Detection Notes**. The note section expands.
4. Click in the note area. If this is the first time a note is added to this detection, click **"Enter any detection notes here"** to place the cursor in the notes area.
5. Click the check icon to save the note. If you want to delete the note, click the delete icon.

Lockdown a Device from Detection Details

You can use the lockdown feature to quickly isolate potentially dangerous or suspicious endpoints. This feature quarantines a compromised (or potentially compromised) endpoint to stop Command and Control (C2) activity, exfiltration of data, or lateral movement of the malware or security attack.

Lockdown disables the network capabilities of the device (LAN and Wi-Fi) to stop it from doing more damage. This gives you time to either investigate the endpoint or physically remove the endpoint from the network.

Note: CylancePROTECT Agent 1440 and later, will display a message on the endpoint when it has been placed in Lockdown mode.

1. In the console, click **CylanceOPTICS**.
2. Click on a detection event to view the Detection Details.
3. On the Detection Details page, click the **Actions** menu.
4. Click **Lockdown Device**. The Device Lockdown settings display. The Actions menu is in the upper-right corner, next to Status.
5. Select the lockdown period. This can be from five minutes up to 96 hours (four days).
6. Click **Confirm Lockdown**.

Export Details to JSON

You can export the detection details as a JSON file.

1. In the console, click **CylanceOPTICS**.
2. Click on a detection event to view the Detection Details.

3. On the Detection Details page, click the **Actions** menu.
4. Click **Export Data**. The detection details JSON file is downloaded.

Use Detection Rule Sets

You can create Detection Rule Sets to meet your organization's needs. To apply a rule set, create or edit a policy and select a rule set under the **CylanceOPTICS Settings** tab in the policy.

1. In the console, click **CylanceOPTICS**.
2. Hover over the **Configuration** tab.
3. Click **Detection Rule Sets**.
4. Click **Create New**.
5. Type a name in the Detection Rule Set Name field. This name must be unique to your organization.
6. Type a description in the Detection Rule Set Description field. This field is optional.
7. Type a message in the Device Notification Message field. This message is displayed by the Agent on the endpoint when the rule set is triggered. This field is optional.
8. Select the Device Policies that the Detection Rule Set will be applied to. This can also be accomplished after creation by following the steps in Apply a Detection Rule Set to a Policy.
9. Select the detections you want to enable. Hover over the information icon to see a short description of the detection.
10. Enable desktop notifications if you want the Device Notification Message to display on the endpoint. Requires CylancePROTECT Agent 1460 or later.
11. Select a Response if you want the Agent to perform an action when the detection event is triggered.
12. Click **Confirm** to view a summary of the rule set. If you need to make any changes to the rule set, click Back, make your changes, then click Confirm.
13. Click **Confirm** to save the rule set.

Apply a Detection Rule Set to a Policy

A detection rule set is applied to your CylanceOPTICS devices using a policy.

1. In the console, select **Settings > Device Policy**.
2. Create or edit a policy.
3. Select **CylanceOPTICS Settings**.
4. Make sure **CylanceOPTICS** is **ON**, then select a detection rule set under Detection Settings.
5. Click **Save**.

   If the endpoint is online, it may take a few minutes for any policy changes to be applied to an endpoint.

   Alternatively, you can associate Detection Rule Sets to Device Policies directly from the Configuration Detection Rule Set page when you create or edit a Detection Rule Set.

Descriptions for Detection Rule Set Options

To view a description for each Detection type, hover over the information icon next to the detection name.

Custom Rules

With custom rules, you can modify the logic of rules provided by Cylance or create your own logic to apply to endpoints using detection rule sets. This functionality allows you to tune existing rules to meet specific environmental needs, as well as use CylanceOPTICS as an additional threat prevention and remediation tool to monitor environments for security threats or anomalous behavior that may only be found in specific, targeted environments. The flexibility of the CAE lets you utilize the logic to monitor for broad behavior characteristics (such as files being created with certain naming patterns) or search for a targeted series of events (such as a process with a certain file signature thumbprint that then creates files and initiates network connections).

These custom rules operate in the same workflows as rules provided by Cylance and can have the same automated response actions to stop malicious activities from occurring the moment CylanceOPTICS identifies them.

View Detection Rules

You can view a list of all CAE behavioral rules and edit, clone, export, or delete the rules from your environment. This is done on the Detection Rules page in the Console.

1. In the console, click **CylanceOPTICS**.
2. Hover over the **Configurations** tab.
3. Select **Detection Rules**.

   The Detection Rules page also allows you to view various details about rules, including their unique identifier, the last time they were modified, who modified the rule, and the number of Detection Rule Sets and Devices to which the rule applies. This data can be easily filtered and exported with the Filter and Export buttons, located in the upper-right corner of the table.

Edit Clone Export and Delete Custom Rules

On the Detection Rules page, you can interact with the rules in various ways, depending on the Category grouping for the rule. The available actions for each category are described in the following table.

Rule Category	Edit	Clone	Export	Delete
Custom	x	x	x	x
Cylance Experimental		x	x	
Cylance Exclusion		x	x	
Cylance macOS Official		x	x	
Cylance Windows Official		x	x	

The **Edit** button is only available for rules in the Custom category because custom rules are unique to your organization. The other rule categories cannot be edited because these are managed by Cylance at a global level to ensure all customers receive and can interact with the same rule logic. You can clone these rules to create one unique to your organization.

The **Custom Rule Editor** allows you to modify various rule details, including the Name, Severity, Applicable Operating Systems, Rule Description, and Rule Logic.

The **Clone** button duplicates the desired rule logic and creates a new instance of the rule, including a new unique identifier. Cloning a rule also uses the Custom Rule Editor for modifying any rule details.

The **Export** button allows you to save the JSON structure of the rule, edit the rule (in a text editor of your choice), and share the rule logic with co-workers and other trusted partners. The JSON structure can then be imported with the Import Rule button on the Detection Rule page.

The **Delete** button allows you to remove rules from the console. Deleting a rule will remove it from any Detection Rule Sets and Devices to which the rule was assigned.

Custom Rule Editor

In the console, CylanceOPTICS has a built-in rule editor for rule creation and modification, without needing to leave the console. You can use the rule editor to fully configure a CAE rule, including the detection rule name, severity, applicable operating systems, the rule description, and the actual JSON structure of the rule.

The JSON editor provides automatic syntactical feedback on the rule's structure and allows you to easily pinpoint areas where the JSON structure is malformed. For example, if a comma, quotation mark, or bracket is missing from the expected location, the JSON editor will display an error and tooltip on the character that is likely missing from the structure. The editor will not allow you to pass the rule into the Validation stage until all syntactical errors are remediated.

The custom rule editor contains a brief help section, with references to a series of knowledge base articles that help explain the structure in which a rule should be written. This can be used as both an onboarding tool for new users, as well as a reference guide for more experienced CylanceOPTICS users.

After you complete all required fields and any syntactical errors have been addressed, you can use the Validate button to compile the rule and pass it through Cylance's rule validator service, which ensures that the rule will be interpreted correctly by CylanceOPTICS endpoints. If the rule does not pass the validation process, you will be presented with an error message detailing the area of the rule that needs to be addressed to successfully pass validation. When the validation process succeeds, you will be presented with a final confirmation page to review the rule details. Once you review the rule, you can press the Publish button to make the rule available in the detection rule sets.

The CylanceOPTICS Sensed Events, Artifacts, and Facets and the CylanceOPTICS Context Analysis Engine Custom Rules are updated with new content as it becomes available, and act as educational and reference material for the various technical functions of the CAE.

Exclusion Rules and Performance Tuning

To address performance degradation issues found in certain environments that generate abnormally high numbers of events (server systems or software engineering systems, for example), the CylanceOPTICS CAE can also be used to exclude events generated by certain processes from being ingested into the CylanceOPTICS data pipeline. By excluding these events from the pipeline, CylanceOPTICS does not need to analyze or record these events into the local database, meaning that there is almost no perceivable performance impact. This feature is useful for tuning CylanceOPTICS to its optimal state within various operating environments.

CylanceOPTICS has a few premade exclusion rules; however, you can use the custom rule editor to write your own exclusions to meet your specific environmental needs. You can write exclusion rules using the same JSON structure as a detection rule; in fact, the goal of the exclusion rule is to successfully satisfy the rule based on processes that need to be excluded. Once the rule is published, you can associate the rule with the whitelist process response action in a detection rule set. With this response action, the Context Analysis Engine will automatically exclude any events and processes that match the associated rule logic.

Note: Enabling an exclusion rule means the processes excluded will no longer be evaluated by the CylanceOPTICS detection engine. While exclusion rules can be used to resolve performance issues on the endpoint, it is important to understand the potential lowering of the overall security of the endpoint.

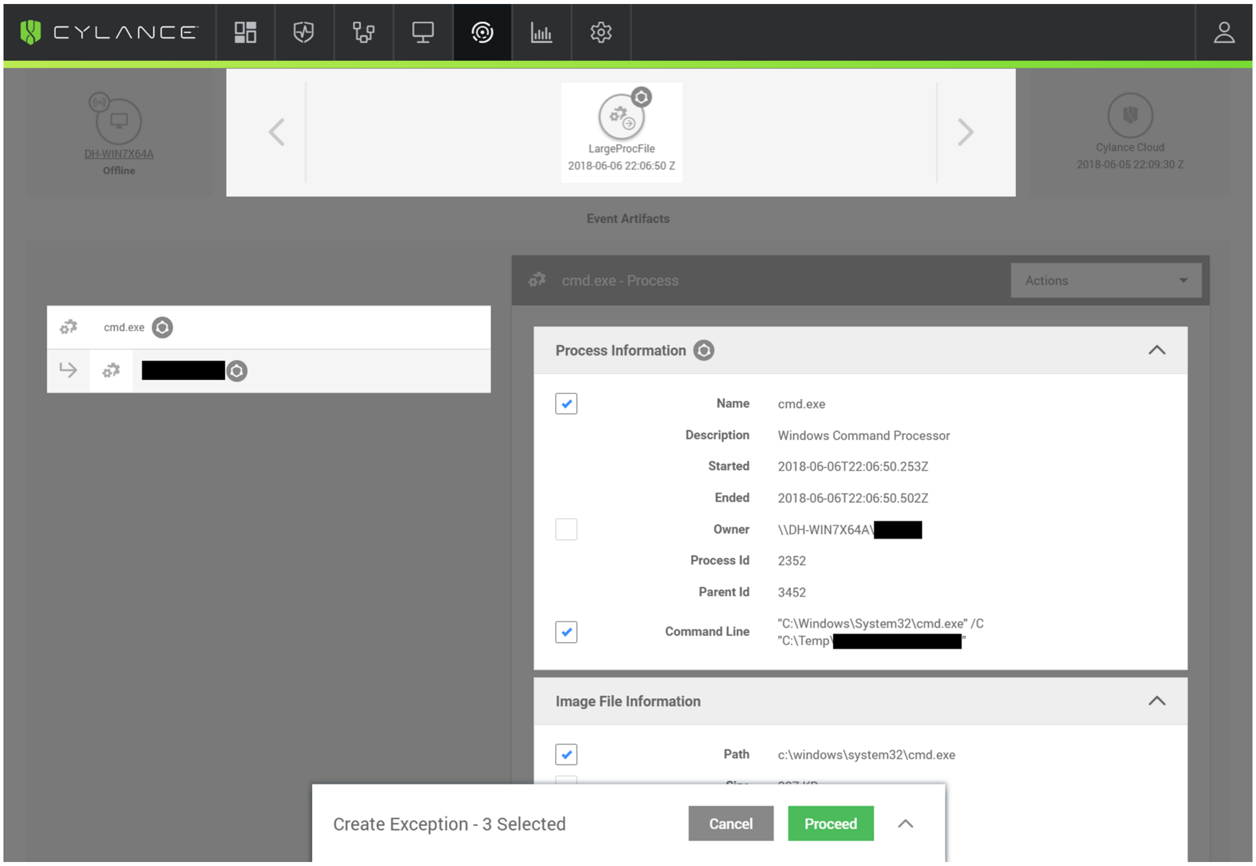
Detection Exceptions

The CylanceOPTICS CAE workflow includes detection exceptions, which allow you to add exceptions to your CAE rules. After you create a detection exception, it can be added to a rule from the Detection Rule Set configuration page. Detection exceptions can also be created from a false positive detection, from the Detection Summary, and the Detection Details pages.

Note: Enabling an exclusion rule means the processes excluded will no longer be evaluated by the CylanceOPTICS detection engine. While exclusion rules can be used to resolve performance issues on the endpoint, it is important to understand the potential lowering of the overall security of the endpoint.

Create a Detection Exception from the Detection Details Page

1. In the console, click **CylanceOPTICS**.
2. For the detection you want to create an exception for, click **View**.
3. Click the **Actions** drop-down, then click **Create Exception**. The Detection Details page updates to highlight information, including artifacts you can add to the exception.
4. Select artifacts you want to include in the exception. In the image below, the exception would check for cmd .exe, running from the Windows path, with a specific command in the command-line argument.



Process Information

☑ Name cmd.exe
Description Windows Command Processor
Started 2018-06-06T22:06:50.253Z
Ended 2018-06-06T22:06:50.502Z
☐ Owner \\DH-WIN7X64A\[redacted]
Process Id 2352
Parent Id 3452
☑ Command Line "C:\Windows\System32\cmd.exe" /C "C:\Temp\[redacted]"

Image File Information

☑ Path c:\windows\system32\cmd.exe

Create Exception - 3 Selected

Cancel Proceed

5. Click **Proceed**. The Create Exception window displays with conditions added, based on the artifacts you selected.
6. Type a name for the detection exception.
7. Add or remove any detection exception conditions.
   a) To add another condition, click the **Add Another Condition** link in the lower-left. Select an Artifact, a Facet, and an Operator. In the Value field, type in the information for the exception.
   b) To remove a condition, click the **Remove** icon (trashcan).
   c) In a Detection Exception, an AND statement is applied to all conditions. This means all conditions must be met for the exception to be true.
   d) The Enter Value field is an ANY statement. When two or more values are added to a condition, if any of these values exist, then this condition is true.
8. Click **Save**. The Exception Saved window displays and includes a message about adding the exception to a Detection Rule Set.
9. To view the Detection Rule Sets page, click the **Detection Rule Sets** link. To close the window, click **Close**.

Create a Detection Exception from the Detection Exceptions Page

1. In the console, click **CylanceOPTICS**.
2. Select **Configurations > Detection Exceptions**.
3. Click **Create Exception**. The Create Exception window displays.
4. Type a name for the detection exception. For example, you can create an exception for a specific command in a command line argument.
5. Add or remove any detection exception conditions.
   a) To add another condition, click the **Add Another Condition** link in the lower-left. Select an Artifact, a Facet, and an Operator. In the Value field, type in the information for the exception.
   b) To remove a condition, click the **Remove** icon (trashcan).
   c) In a Detection Exception, an AND statement is applied to all conditions. This means all conditions must be met for the exception to be true.
   d) The Enter Value field is an ANY statement. When two or more values are added to a condition, if any of these values exist, then this condition is true.
6. Click **Save**. The Exception Saved window displays and includes a message about adding the exception to a Detection Rule Set.
7. To view the Detection Rule Sets page, click the **Detection Rule Sets** link. To close the window, click **Close**.

Add Exception to Detection Rule Set

1. In the console, click **CylanceOPTICS**.
2. For the rule set to add the exception to, click the **Edit** icon.
3. Expand the rule set that contains the rule to add the exception.
4. Under Exceptions, in the drop-down list, then select the Detection Exceptions you want to add. You can select more than one exception to add to the rule.
5. Click **Confirm**. A summary page displays.
6. Click **Save**.

False Positive Detections

You can mark one or more events that you have verified as a false positive. Using the False Positive status allows you to filter these detections.

Changing the Status on the Detections Page

1. In the console, click **CylanceOPTICS**.
2. For the false positive detection, in the **Status** drop-down list click **False Positive**. The False Positive window displays with all duplicate detections selected.
3. Select a Clean-up Duplicate False Positives option:
   a) **Mark only this Detection as False Positive**: For the detection you selected in the previous step, this will change the status to False Positive for that detection. If duplicate detections are selected, the status for these detections is not changed.
   b) **Mark all Selected Detections as False Positive**: For the detection you selected, and all duplicates identified, this will change the status to False Positive and remove these detections from the Detections page.
   c) **Mark all Selected Detections as False Positive and Delete**: For the detection you selected, and all duplicates identified, this will change the status to False Positive and remove these detections from the Detections page.
4. Click **Save**.

Changing the Status on the Detection Details Page

1. In the console, click **CylanceOPTICS**.
2. For the false positive detection, click the **View**. The Detection Details page displays for the selected detection.
3. In the **Status** drop-down list click **False Positive**. The False Positive window displays with all duplicate detections selected.
4. Select a Clean-up Duplicate False Positives option:
   a) **Mark only this Detection as False Positive**: For the detection you selected in the previous step, this will change the status to False Positive for that detection. If duplicate detections are selected, the status for these detections is not changed.
   b) **Mark all Selected Detections as False Positive**: For the detection you selected, and all duplicates identified, this will change the status to False Positive and remove these detections from the Detections page.
   c) **Mark all Selected Detections as False Positive and Delete**: For the detection you selected, and all duplicates identified, this will change the status to False Positive and remove these detections from the Detections page.
5. Click **Save**.

Detection Rule Set Best Practices

A simple best practice workflow for Detection Rule Sets is:

1. Enable rules in Alert-only mode. Enable the rule, but do not enable Responses or Notifications. This will show you what is triggered in your environment, including any false positives.
2. Review events and create Exceptions (if necessary). Creating Detection Exceptions helps eliminate false positives and duplicate events. See the Detection Exceptions section for more information.
3. When reviewing events and creating Exceptions is complete, enable Responses to the rules. Optionally, enable Notifications.

Note: Enabling an exclusion rule means the processes excluded will no longer be evaluated by the CylanceOPTICS detection engine. While exclusion rules can be used to resolve performance issues on the endpoint, it is important to understand the potential lowering of the overall security of the endpoint.

Package Playbook

Currently, refract packages must be run using the user-interface or an API call. This creates a situation where there can be a potentially significant lag time between when an incident occurs, and an analyst or incident responder is able to send a package execution command to affected endpoints. The lag time introduced by this could lead to gaps in critical forensic information relevant to an incident investigation.

Package playbooks implement a mechanism to automatically execute refract packages on endpoints as part of the automated response action framework, such that users on Cylance's products can configure their detection rule sets to execute a specified set of refract packages upon the successful trigger of a single or multiple Context Analysis Engine rules.

About Package Playbooks

- A package playbook is a group of refract packages (Cylance packages and custom packages).
- A package playbook can contain up to 20 packages.
- A tenant can have up to 100 package playbooks.
- A package playbook cannot be added to another package playbook.
- You can apply up to 10 package playbooks per detection rule.
- Package playbook content is stored on the endpoint; this allows execution even if the endpoint is offline.
- Package playbook execution will not interfere with more immediate response actions, like terminate process, suspend process, delete files, and logoff users.
- Using a package playbook allows administrators to change one playbook and have it affect all detection rules associated with that playbook.

Create a Package Playbook

1. In the Console, select **CylanceOPTICS**.
2. Select **Configurations > Package Playbooks**.
3. Click **Create Playbook**.
4. Type a name for the playbook.
5. Optionally, type a description. This can state the purpose of the playbook and help identify it for use when adding it to a Detection Rule Set.
6. Select a **Collection Type**. This is where the files are saved. By default, the files are saved on the endpoint.
7. Add a package to the playbook. Click **Add Another Package** to add more packages to the playbook.
8. Optionally, type in a command-line argument to use with the selected package.
9. Click **Save**.

Clone a Package Playbook

Cloning a Package Playbook allows you to keep the original and modify a clone to suit your needs.

1. In the Console, select **CylanceOPTICS**.
2. Select **Configuration > Package Playbooks**.
3. For the playbook you want to duplicate, click **Clone**.
4. Type a name for the playbook. By default, **(clone)** is added to the end of the existing name.

Note: For remote collection types (for example, SFTP), a password or key is required. You can change the Collection Type to Local, which does not require a password or key.

5. Click **Next**.
6. Add or remove packages. Add optional command line arguments.
7. Click **Save**.

Associate a Package Playbook with a Detection Rule

1. In the Console, select **CylanceOPTICS**.
2. Select **Configuration > Detection Rule Sets**.
3. Create or edit a rule set.
4. Expand a rule set. For each rule within a set, you should see Exceptions, Response, and Playbooks as drop-down lists.
5. Select a playbook to associate it with a rule.
6. Click **Confirm**.

Package Playbook Execution Confirmation

If a Detection Rule triggers the execution of a Package Playbook, the Detection Details page of the event will show a confirmation.

Package Playbook Endpoint Behavior

When a Detection Rule triggers and it has a Package Playbook associated to it, the Playbook will begin to execute on the endpoint and run all the associated Packages. The results will be uploaded to the defined collection location once the execution has finished.

Deploy a package to collect data from devices

You can use the Optics package deploy feature to remotely and securely run a process (for example, a Python script) on Optics devices to collect and store desired data in a specified location for further analysis by security administrators. For example, you can run a process to collect browser data. You can use the Optics data collection packages that are available in the management console or you can create your own.

When you deploy a package to devices that are offline, the deployment will wait for those devices to come online for a specified period.

Before you begin:

- If desired, create a package that will execute on a device, collect specific data points, and output that data to a local or server location that you will specify in the steps below. For more information about creating a custom package, visit support.blackberry.com/community to read article 66563.
- If you create your own package, you must upload it to the management console. In the console, go to **CylanceOPTICS > Configurations**, hover over **Configurations** and click **Packages**, then click **Upload file**.

1. In the management console, on the menu bar, click **CylanceOPTICS > Packages**.
2. lick **Deploy Packages**.
3. In the **Package** drop-down list, click the package that you want to send to devices. Click **Add Another Package** to add additional packages.
4. In the **Collection Type** drop-down list, click the location where you want to store the data that the package will collect.
    - **Local** saves the data at the indicated path on the device.
    - If you select **SFTP**, **SMB**, or **S3**, specify the required information.
5. Click **Next**.
6. Select **Device** or **Zone** and select the devices or zones that you want to deliver the package to.
7. If you want to specify a timeout period and priority for the package deploy, click **Show advanced options** and do any of the following:
    - In the **Valid for** drop-down list, click the desired timeout period. If a device is not online within this period, the package deploy is cancelled for that device.
    - Adjust the **Priority** slider to set a higher or lower priority. The priority is taken into account when other Optics jobs are queued for the same device.
8. Specify a name and description for the package deploy.
9. Click **Deploy**.

After you finish:

- Navigate to **CylanceOPTICS > Packages** to view the current status and progress of the package deploy.
- You can click a package deploy status to view details about the deploy. You can expand the Targets section to view the individual status of each device. If you want to stop a package deploy that is in progress, in the **Select Action** drop-down list, click **Stop Job**.

Locking Down an Endpoint

With CylanceOPTICS, administrators can quickly isolate an infected (or potentially infected) endpoint to stop command and control (C2) activity, exfiltration of data, or lateral movement of malware. The CylanceOPTICS lockdown feature gives administrators time to investigate the endpoint or physically remove the endpoint 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. You can use an unlock key to unlock a device before the lockdown period ends. See Unlock an Endpoint.

Note: The Lockdown Device feature is currently not available for the CylanceOPTICS Linux Agent.

About Lockdown

- When an endpoint lockdown period has expired, it can take up to two minutes for that endpoint to display as connected on the Devices page.
- CylancePROTECT Agent 1440 and later will display a notification on the endpoint when it has been placed into a lockdown.

Lockdown an Endpoint

1. In the console, select **CylanceOPTICS**.
2. Select **Devices**. A list of endpoints displays. Search for a device name to filter the list.
3. Click the **Actions** menu.
4. Click **Lockdown Device**. The Lockdown - Network Isolation window displays.
5. Select a lockdown period. This can range from five minutes up to 96 hours.
6. Click **Confirm Lockdown**. The endpoint status shows that it is locked down and the duration before the endpoint is automatically unlocked.

   Once an endpoint is locked down, the CylanceOPTICS status column displays a red icon.

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

Unlock an Endpoint

Unlocking an endpoint, before the lockdown expires, is a manual process. This manual process requires direct access to the endpoint and the unlock key.

1. In the console, select **CylanceOPTICS**.
2. Select **Devices**.
3. Search for and select the device to unlock.
4. Click the **Actions** menu.
5. Click **Show Unlock Key**. Use this key on the locked down endpoint. Each unlock key is unique to each locked down endpoint.
6. On the endpoint, start an administrator Command Prompt and type in the following:

   - **For Windows:**

    - Navigate to the CylanceOPTICS executable folder. The default location for CyOptics.exe is: `C:\Program Files\Cylance\Optics`
    - `CyOptics.exe control --password "unlock_key" unlock -a`
    - Replace `"unlock_key"` with the Unlock Key in step 5.
- **For macOS:**
    - `cd /Library/Application\ Supprt/Cylance/Optics/CyOptics.app/Contents/Resources`
    - `sudo ../MacOS/CyOptics control --password 'OpticsPassword' unlock -net`
    - Replace `'OpticsPassword'` with the Unlock Key in step 5.

Remote Response

Remote response provides Cylance Console administrators with an interface to execute scripts and run commands on the device. Administrators can triage a system and see the results from within the Cylance Console.

Secure Communications

Remote response uses the same secure technology that allows the Cylance Console to communicate with the Cylance Agent, allowing administrators to run commands on the device, no matter where the device is (so long as the device can communicate with the Console).

How it Works

When using remote response, the CylanceOPTICS Agent will spawn an instance of the device's native terminal or shell (cmd for Windows, bash for macOS and Linux) and transport to and from the Console into the terminal or shell. By allowing administrators to interact with the native shell, they have access to all native functions of that shell as well as access to applications or scripts that are already on the device.

Remote Response also includes two custom, cross-platform commands: rr-put and rr-get. These can transfer files to and from the device.

Operating Systems Supported

Remote Response works on all operating systems that CylanceOPTICS supports (Windows, macOS, and Linux).

Audit Logs

Due to the high level of access granted by Remote Response, a full session audit log is generated and exposed for all commands sent to an device, as well as the responses that are returned for the device.

Note:

- Remote Response grants a high-level of access to the device. Administrators must use caution when issuing commands so the device is not negatively impacted or damaged. Cylance is not responsible for the actions of an organization's administrators.
- The organization's administrators must know the device's operating system and the commands available to that OS. Cylance will not provide assistance for this.

Things to Know

- Remote Response requires CylanceOPTICS version 2.5.0 or higher.
- Remote Response is available to Console administrators only.
- Remote Response logs are retained for 90 days.
- Remote Response session will time out after 25 minutes of inactivity.
- An administrator can have up to 10 Remote Response sessions at a time.
- Up to 50 Remote Response sessions for a single device. This allows multiple administrators to investigate the same device.
- Send or receive up to 70 MB per command. This applies to rr-get and rr-put. Attempting to send or receive a file larger than 70 MB results in an error message.

Why Remote Response is not Available for a Device

Remote response may not be available for a device for the following reasons:

- Device is not running CylanceOPTICS version 2.5.0 or higher.
- The device is not online (not connected to the Console).

- The administrator already has a Remote Response session open.

Using Remote Response

1. In the Console, select **CylanceOPTICS > Devices**. A list of CylanceOPTICS devices displays.
2. Click on the Device name to display the Device Drawer.
3. Click **Select Action > Remote Response**. The CylanceOPTICS Remote Response Session window opens. The Remote Response session windows displays:
    - The device name
    - Operating system
    - Disk usage
    - Memory usage
    - Uptime (the number of days, hours, and minutes the Agent has been running without a system or service
4. Enter commands into the Remote Response Session window. You can copy/paste commands into the window.

Remote Response Terminal

The top-right corner of the Remote Response Terminal window includes three controls:

- Maximize the window. This is the broken square icon.
- Minimize the window. This is the down arrow.
- Close the window. This is the x icon. Attempting to close the window displays a message asking for confirmation. When you confirm the message, all active Remote Response sessions will be disconnected and the Remote Response Terminal window will be closed.

Reserved Commands

Remote Response has five reserved commands that do not interact directly with the native shell on the device. These commands provide a uniform cross-platform experience for some common actions.

Command	Description
rr-clear	Clears the text in the Remote Response Terminal window.
rr-get	Use rr-get followed by an absolute path (including the file name) and Remote Response will copy the file from the device and download it to the administrator's web browser. The administrator will be able to choose where the file will be saved on their local system. **Example:** rr-get C:\Program Files\Cylance\Desktop\2020-03-26.log
rr-help	Displays a list of all Remote Response reserved commands, along with a short description of each command.

Command	Description
rr-put	Use rr-put followed by a path to a directory (without a file name) and Remote Response will open a file browser window. The administrator can select the file they want to send to the device. Remote Response will automatically populate the file name when it is selected. A copy of the file is sent directly from the administrator's file browser to the device. **Example:** rr-put C:\Users\username\Downloads (this will put the file you select into the device user's Downloads folder). **Note:** The file content is not stored in the Cylance Cloud. A record of the command being executed will be in the Remote Response audit log, but not file content is saved in the log.
rr-quit	Disconnects the Remote Response session. The Remote Response Terminal window remains open, allowing the administrator to view the session history, but no further commands will be sent or received.

Examples of Remote Response

Note: The following examples used a Windows 10 device.

Using rr-put

This example will show how to copy a file (HelloWorld.txt) to the device.

1. Create a text file that includes content. This example uses HelloWorld.txt for the file name and Hello World for the content. An empty file (0 KB) cannot be sent using rr-put.
2. In the Console, select **CylanceOPTICS > Devices**.
3. Click the device name. The Device Drawer displays.
4. Select **Select Action > Remote Response**.
5. Type `rr-put C:\`, then press **Enter**. A file browser opens.
6. Select the HelloWorld.txt file, then click **Open**. Or select the file you want to copy to the device. The file browser closes and the file name appears in the command line.
7. Press **Enter**. The file is sent to the device. A percentage of completion displays, and then a `Transfer complete` when the file transfer completes successfully.

Deleting the HelloWorld File

1. Create a text file that includes content. This example uses HelloWorld.txt for the file name and Hello World for the content. An empty file (0 KB) cannot be sent using rr-put.
2. In the Console, select **CylanceOPTICS > Devices**.
3. Click the device name. The Device Drawer displays.
4. Select **Select Action > Remote Response**.
5. Type `del "C:\HelloWorld.txt"`, then press **Enter**. Include the quotation marks around the file path and file name. The file is deleted from the device.

Using rr-get

This example will show how to copy a CylanceOPTICS log file from the device.

1. In the Console, select **CylanceOPTICS > Devices**.
2. Click the device name. The Device Drawer displays.
3. Select **Select Action > Remote Response**.
4. Type rr-get C:\ProgramData\Cylance\Optics\Log\Optics-2020-03-27.csv. You can change the date in the file name to retrieve a log file.
5. Press **Enter**. The log file is downloaded to your system via the web browser.

Download Remote Response Audit Logs

Note: A Remote Response audit log will display as Not Available when a session is still active.

1. In the Console, select **CylanceOPTICS > Action History > Remote Response Logs**.
2. Click **Download Log** for the log you want to view.
3. Extract the log from the .gz file.
4. Open the log file using a text editor.
5. The log contains Remote Response information, device information, and the commands used during this session.

Remote Response Log Descriptions

Name	Description
Commands	This is the number of commands issued during this session.
Device	This is the name of the device.
Download	This is the link to download the audit log. Remote Response Logs are compressed as GZ files.
Session End	This is the date and time the Remote Response session ended. If this is blank, then the session is still open.
Session Start	This is the date and time the Remote Response session was started.
Session User	This is the email address of the administrator who used Remote Response.

Context Analysis Engine Custom Rule Builder

The CylanceOPTICS Context Analysis Engine Custom Rule Builder allows users to extend the logic of behavioral rules provided by Cylance as well as the ability to create their own logic to detect malicious or suspicious behaviors in their own environments.

Note: User imported custom rules are not supported by Cylance Support.

The Context Analysis Engine (CAE) rules consist of five primary pieces of data:

- **States**: States define the flow of a CAE Rule. These allow CylanceOPTICS to statefully observe a series of Events that occur on a device. These represent a "**1, then 2, then 3**" scenario that might occur.
- **Functions**: Functions define the logic required to successfully fulfill a State. This logic applies directly to the defined field operators and is used to represent a "**A, and B, and C**" or "**A, and B, but not C** attributes of an Event that occurs on a device.
- **Field Operators**: Field operators define how operands (facet value extractors) are evaluated. Field operators include actions like Equals, Contains, and Is True.
- **Operands (Facet Value Extractors)**: Operands act as the values being compared by CylanceOPTICS. Operands allow extracting specific pieces of data about an Event on a device (like File Paths, File Hashes, and Process Names) and compare those with literal values (like String, Decimal, Boolean, and Integer).
- **Artifacts of Interest (AOI)**: AOI define the points where CylanceOPTICS can interact with a rule to take automated response actions. These artifacts are targeted by CylanceOPTICS when conducting actions such as Terminating Processes, Logging Off Users, or Deleting Files.
- **Paths**: Paths define how the CAE interprets the flow of multiple state objects within a rule.

Sample Rule

```
{
    "States": [
    {
        "Name": "TestFile",
        "Scope": "Global",
        "Function": "(a)",
        "FieldOperators": {
            "a": {
                "Type": "Contains",
                "Operands": [
                    {
                        "Source": "TargetFile",
                        "Data": "Path"
                    },
                    {
                        "Source": "Literal",
                        "Data": "my_test_file"
                    }
                ],
                "OperandType": "String"
                }
            },
            "ActivationTimeLimit": "-0:00:00.001",
            "Actions": [
                {
                    "Type": "AOI",
                    "ItemName": "InstigatingProcess",
                    "Position": "PostActivation"
                },
                {
                    "Type": "AOI",
                    "ItemName": "TargetProcess",
                    "Position": "PostActivation"
                },
                {
                    "Type": "AOI",
                    "ItemName": "TargetFile",
                    "Position": "PostActivation"
                }
            ],
            "HarvestContributingEvent": true,
            "Filters": [
                {
                    "Type": "Event",
                    "Data": {
                        "Category": "File",
                        "SubCategory": "",
                        "Type": "Create"
                    }
                }
            ]
        }
    ],
     "Paths": [
        {
            "StateNames": [
            "NewSuspiciousFile",
            "CertUtilDecode"
            ]
        }
    ],
    "Tags": [
        "CylanceOPTICS"
    ]
}
```

States

States are the highest logic level of a Context Analysis Engine (CAE) rule and have a larger number of required fields.

Field Name	Description
Actions	This field contains a list of objects used to define Artifacts of Interest within a state. See Artifacts of Interest for more information.
ActivationTimeLimit	This field defines how long CylanceOPTICS will wait for events to trigger the event. This should be the default value of -0:00:00:001.
FieldOperators	This is an object that contains the field operators and operands that should be inspected to fulfill the function defined in the state. See Field Operators for more information.

Field Name	Description
Filters	This field defines which event categories, subcategories, and types that CylanceOPTICS should inspect when attempting to fulfill a State. See Filters for more information.
Function	This field contains the logic function that CylanceOPTICS must observe to consider a state as satisfied. See Functions for more information.
HarvestContributingEvents	This field defines whether or not CylanceOPTICS should record the events that satisfy a state. The value should be set to true.
Name	This field defines the name of the state that will be displayed in the UI should the rule become satisfied.
Scope	This field defines the scope in which CylanceOPTICS looks for relevant events. In most cases, this field should remain set to global.
States	This field contains a list of one or more state objects. These objects can be chained.

Functions

Functions define the logic required to successfully fulfill a State for a Context Analysis Engine (CAE) rule. This logic applies directly to the defined field operators and is used to represent an A, and B, and C or A, and B, but not C attributes of an event that occurs on a device. This logic applies directly to the defined field operators within a state.

Function	Description	Example
AND - &	Two or more field operators must be matched to consider the state satisfied.	a & b & c
OR - |	One of two or more field operators must be matched to consider the state satisfied.	a | b | c
NOT - !	A defined field operator must be False or Not Matched to consider the state satisfied.	a & b & !c
GROUP - ()	Field operators are grouped together to fulfill more complex logic requirements.	(a & b) | (c & !d)

Field Operators

Field Operators are the logical pieces of a rule that allow CylanceOPTICS to compare two values. If there are two or more operands, and they match the comparison criteria, CylanceOPTICS will consider that portion of the defined function as complete. When all pieces of the function are complete, the state will be satisfied.

The field operators field is an object that will consist of one or more conditional objects. These conditional objects can be set to any value, however, they must match the same conditional values that are referenced in the function field. As such, BlackBerry recommends that these names are kept to simple and logical values, such as numbers or letters.

Field Operator	Description
ContainsAll	Determines if the specified operand contains all of the operands from a set Positive: "hello, I am a string" contains all from ("ello", "ng") Negative: "hello, I am a string" does not contain all from ("hi", "ng")
ContainsAllWords	Determines if the specified operand contains all of the operands from a set, where each set operand must appear as a whole word surrounded by white space, punctuation, or end/beginning string markers Positive: "hello, I am a string" contains all words from ("hello", "a", "string") Negative: "hello, I am a string" does not contain all words from ("ello", "ng")
Contains	Determines if the specified operand contains any of the operands from a set Positive: "hello, I am a string" contains any from ("ello", "banana") Negative: "hello, I am a string" does not contain any from ("hi", "banana")
ContainsWord	Determines if the specified operand contains any of the operands from a set, where each set operand would have to appear as a whole word surrounded by white space, punctuation, or end/beginning string markers Positive: "hello, I am a string" contains any words from ("hello", "banana") Negative: "hello, I am a string" does not contain any words from ("ello", "ng")
EndsWith	Determines if the specified left operand ends with the specified right operand Positive: "hello, I am a string" ends with "ring" Negative: "hello, I am a string" does not end with "bring"
Equals	Determines if the specified operand equals exactly any of the operands from a set, where each set operand would have to appear as a number or a whole word surrounded by white space, punctuation, or end/beginning string markers Positive: 10 equals any from (10, 20, 30) Positive: "hello" equals any from ("hello", "banana") Negative: 100 does not equal any from (10, 20, 30) Negative: "hello" does not equal any from ("ello", "ng")
GreaterThan	Determines if the specified left operand is greater than the specified right operand Positive: 14.4 is greater than 10.1 Negative: 1 is not greater than 1000

Field Operator	Description
GreaterThanOrEquals	Determines if the specified left operand is greater than or equal to the specified right operand Positive: 14.4 is greater than or equal to 10.1 Negative: 1 is not greater than or equal to 1000
InRange	Determines if the specified middle operand is between the left and right operands Positive: 10 is between 1 and 20 Positive: 5.3 is between 5.3 and 20.1 (inclusive) Negative: 4 is not between 5 and 10 Negative: 20 is not between 20 and 40 (exclusive)

<table>
<tr><th>Field Operator</th><th>Description</th></tr>
<tr><td>IpIsInRange</td><td>

Determines if the TargetNetworkConnection address (SourceAddress, DestinationAddress) is within the specified "min" and "max" options

Allowed Operands are:

```
{
    "Source": "TargetNetworkConnection",
    "Data": "SourceAddress"
}
```

And:

```
{
    "Source": "TargetNetworkConnection",
    "Data": "DestinationAddress"
}
```

Example:

```
"FieldOperators": {
    "a": {
        "Type": "IpIsInRange",
        "OperandType": "IPAddres",
        "Options": {
            "min": "123.45.67.89",
            "max": "123.45.67.255"
        },
        "Operands": [
            {
                "Source": "TargetNetworkConnection",
                "Data": "DestAddr"
            }
        ]
    }
}
```

Include the following Filters object with the above example to output the network traffic

```
"Filters": [
    {
        "Type": "Event",
        "Data": {
            "Category": "Network",
            "SubCategory": "*",
            "Type": "Connect"
        }
    }
]
```

</td></tr>
</table>

Field Operator	Description
IsHomoglyph	Determines if the left operand is a homoglyph of the right operand. Homoglyphs are things that appear to have the same meaning visually, but are actually different For example, a US Latin 1 "e" and a French "e" appear to be the same character and have the same meaning, but the computer sees them as different values Positive: "3xplor3" is a homoglyph of "explore" with 100% certainty Positive: "3xplord" is a homoglyph of "explore" with 90% certainty Negative: "temp" is not a homoglyph of "temp" because these are the same string Negative: "431" is not a homoglyph of "big" because these share no transitive characteristics
IsNullOrEmpty	Determines if the specified operand is null or empty Positive: <null> is null or empty Positive: "" is null or empty Positive: " " is null or empty Negative: "Hello" is not null or empty
IsPopulated	Determines if the specified operand is not null or empty Positive: "Hello" is not null or empty Negative: <null> is null or empty Negative: "" is null or empty Negative: " " is null or empty
IsTrue	Determines if the specified value is True Positive: TriState.True Negative: TriState.False Negative: TriState.Unknown
LessThan	Determines if the specified left operand is less than the specified right operand Positive: 4.4 is less than 10.1 Negative: 1000 is not less than 1
LessThanOrEquals	Determines if the specified left operand is less than or equal to the specified right operand Positive: 4.4 is less than or equal to 10.1 Positive: 14 is less than or equal to 14 Negative: 1000 is not less than or equal to 1

Field Operator	Description
LevenshteinDistance	Determines if the distance, the number of changes needed to turn one operand into another operand, is within an acceptable range Positive: "cat" is within a Levenshtein Distance of 1 from "bat" Positive: "hello" is within a Levenshtein Distance of 3 from "bell" Negative: "cart" is not within a Levenshtein Distance of 1 from "act"
RegexMatches	Determines if the specified operand conforms to a regular expression Positive: "hello, I am a string" conforms to "^hello, [Ii] am [aA] string$" Negative: "hello, I am a string" does not conform to "^[hi\|hey], I am a string$"
StartsWith	Determines if the specified left operand starts with the specified right operand Positive: "hello, I am a string" starts with "hello, I" Negative: "hello, I am a string" does not start with "help"

Operands - Facet Value Extractors

Facet value extractors are utilized by the CylanceOPTICS CAE to identify an individual property (facet) of a single artifact that was associated with an event that was observed by CylanceOPTICS. While facet value extractors are narrowly scoped by themselves, they can be strung together in a logical way to analyze complex behaviors that are occurring on a device and trigger a detection event in CylanceOPTICS.

Extractor Name	Description	Supported Facets
InstigatingProcess	Extracts a facet from the instigating process of an event. This is commonly used to inspect the name or command line arguments of a process initiating an action (like starting another process, initiating a network connection, or writing a file).	Name (as String) CommandLine (as String)

Extractor Name	Description	Supported Facets	
InstigatingProcessImageFile	Extracts a facet from the image file associated with the instigating process of an event. This is commonly used to inspect various attributes of the image file used to launch a process such as its name, path, hash, or signature status.	Path (as String) Size (as Integer) Md5Hash (as String) Sha256Hash (as String) IsHidden (as Boolean) IsReadOnly (as Boolean) Directory (as String) SuspectedFileType (as String) SignatureStatus (as String) IsSelfSigned (as Boolean) LeafDNSString (as String) LeafThumbprint (as String) LeafSignatureAlgorithm (as String) LeafCN (as String) LeafDN (as String) LeafOU (as String) LeafO (as String) LeafL (as String) LeafC (as String)	IssuerDNString (as String) IssuerThumbprint (as String) IssuerSignatureAlgorithm (as String) IssuerCN (as String) IssuerDN (as String) IssuerOU (as String) IssuerO (as String) IssuerL (as String) IssuerC (as String) RootDNString (as String) RootThumbprint (as String) RootSignatureAlgorithm (as String) RootCN (as String) RootDN (as String) RootOU (as String) RootO (as String) RootL (as String) RootC (as String)
InstigatingProcessOwner	Extracts a facet from the owner associated with the instigating process of an event. This is commonly used to inspect the user who owns the running process.	Name (as String) Domain (as String)	

Extractor Name	Description	Supported Facets
TargetFile	Extracts a facet from the file upon which an event occurred. This is commonly used to inspect various attributes of the file that is being acted upon such as its name, path, hash, or signature status.	See InstigatingProcessImageFile.
TargetFileOwner	Extracts a facet from the owner associated with the file upon which an event occurred. This is commonly used to inspect the user who owns the file being acted upon.	See InstigatingProcessOwner.
TargetNetworkConnection	Extracts a facet from the network connection upon which an event occurred. This is commonly used to inspect the network IP address or port that is being acted upon.	SourceAddress (as IPAddress) SourcePort (as Integer) DestinationAddress (as IPAddress) DestinationPort (as Integer)
TargetProcess	Extracts a facet from the process upon which an event occurred. This is commonly used to inspect the name or command line arguments of a process being acted upon (like process being started or terminated).	See InstigatingProcess.
TargetProcessImageFile	Extracts a facet from the image file associated with a process upon which an event occurred. This is commonly used to inspect various attributes of the image file used to launch a process such as its name, path, hash, or signature status.	See InstigatingProcessImageFile.

Extractor Name	Description	Supported Facets
TargetProcessOwner	Extracts a facet from the owner associated with a process upon which an event occurred. This is commonly used to inspect the user who owns the process being acted upon.	See InstigatingProcessOwner.
TargetRegistryKey	Extracts a facet from the registry key upon which an event occurred. This is commonly used to inspect the registry key or value that is being acted upon.	Path (as String) ValueName (as String)

Path Value Extractors

Extractor Name	Description
EnvVar	Extracts an environment variable from the Operating System
LiteralWithEnvVar	Expands a path that contains an environment variable
Literal	Represents a literal value. This is the most common extractor and operand

Artifacts of Interest

The Artifacts of Interest (AOI) in the Actions field allows users to define a list of artifacts that can allow CylanceOPTICS to enact automated response actions against. The Artifacts of Interest (AOI) that are able to be defined here follow the same syntax as the operands defined in the previous section. It should also be noted that any artifact associated with an event or set of events that satisfy a state can be marked as an AOI. AOI do not need to be defined as an operand to be considered an AOI.

In the case that a filter is applied to a state, users should be aware that some AOI will not be available to take automatic response actions against. For example, if a File Create Filter is applied to a state, users will implicitly have file and process related AOI available but would not have registry or network related AOI. In the event that an irrelevant AOI is provided in a state, the CylanceOPTICS Agent will gracefully handle its exclusion. The table below outlines the applicable filter to AOI relationships.

Category	Subcategory	Type	Applicable AOI
File		Create	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetFile TargetFileOwner
File		Delete	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetFile TargetFileOwner
File		Rename	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetFile TargetFileOwner
File		Write	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetFile TargetFileOwner
Network	IPv4	Connect	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetNetworkConnection
Network	IPv6	Connect	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetNetworkConnection
Network	TCP	Connect	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetNetworkConnection

Category	Subcategory	Type	Applicable AOI
Network	UDP	Connect	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetNetworkConnection
Process		Exit	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetProcess TargetProcessImageFile TargetProcessOwner
Process		Start	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetProcess TargetProcessImageFile TargetProcessOwner
Process	CylancePROTECT	AbnormalExit	TargetProcess TargetProcessImageFile TargetProcessOwner
Registry		PersistencePoint: KeyCreating	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetRegistryKey
Registry		PersistencePoint: KeyCreated	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetRegistryKey
Registry		PersistencePoint: KeyDeleting	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetRegistryKey

Category	Subcategory	Type	Applicable AOI
Registry		PersistencePoint: KeyDeleted	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetRegistryKey
Registry		PersistencePoint: KeyRenaming	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetRegistryKey
Registry		PersistencePoint: KeyRenamed	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetRegistryKey
Registry		PersistencePoint: ValueChanging	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetRegistryKey
Registry		PersistencePoint: ValueChanged	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetRegistryKey
Registry		PersistencePoint: ValueDeleting	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetRegistryKey
Registry		PersistencePoint: ValueDeleted	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetRegistryKey

Category	Subcategory	Type	Applicable AOI
Thread		Create	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetProcess TargetProcessImageFile TargetProcessOwner
Thread		Inject	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetProcess TargetProcessImageFile TargetProcessOwner

Example of Actions:

```
"Actions": [
    {
        "Type": "AOI",
        "ItemName": "InstigatingProcess",
        "Position": "PostActivation"
    },
    {
        "Type": "AOI",
        "ItemName": "TargetProcess",
        "Position": "PostActivation"
    },
    {
        "Type": "AOI",
        "ItemName": "InstigatingProcessOwner",
        "Position": "PostActivation"
    }
],
```

Paths

Paths define how the Context Analysis Engine (CAE) interprets the flow of multiple State objects within a rule. Paths are used when a rule is created that consists of multiple state objects (also known as a multistate rule). States define the flow of a CAE rule. These allow CylanceOPTICS to statefully observe a series of events that occur on an endpoint. These represent a "1, then 2, then 3" scenario that might occur.

Note: If a rule has only one State object, there is no need to use a Paths object. Cylance rules consist of a single State object and do not explicitly require the use of the Paths object. Cylance rules that do utilize the Paths object do so only for explicit definition (not for rule functionality).

In the following examples, two state objects are used, NewSuspiciousFile and CertUtilDecode. Each state has its own set of logic.

Example 1: In the following configuration, the CAE will look for an event that satisfies the NewSuspiciousFile state. Once that state is satisfied, the CAE will look for an event that satisfies the CertUtilDecode state.

```
"Paths": [
    {
        "StateNames": [
            "NewSuspiciousFile",
            "CertUtilDecode"
        ]
    }
],
```

Example 2: In the following configuration, the CAE will look for an event that satisfies the CertUtilDecode state, then the NewSuspiciousFile state.

```
"Paths": [
    {
        "StateNames": [
            "CertUtilDecode",
            "NewSuspiciousFile"
        ]
    }
],
```

Example 3: In the following configuration, the CAE will look for an event that satisfies the NewSuspiciousFile state or the CertUtilDecode state. This is helpful when states have different filter object sets. In this example, NewSuspiciousFile uses a File Write filter and CertUtilDecode uses a process Start filter.

```
"Paths": [
    {
        "StateNames": [
            "CertUtilDecode"
        ]
    },
    {
        "StateNames": [
            "NewSuspiciousFile"
        ]
    }
],
```

Filters

Filters allow the scope of a state to be narrowed or expanded to account for a smaller or larger number of events to analyze. Event filters utilize the same event categories, subcategories, and types that are outlined in the CylanceOPTICS sensed events and artifacts.

Example 1:

A user wanting to limit inspected events to process start events could structure their filter section to look like the following.

```
"Filters": [
    {
        "Type": "Event",
        "Data": {
            "Category": "Process",
            "SubCategory": "",
            "Type": "Start"
        }
    }
]
```

Example 2:

Whereas a user wanting to inspect all types of file events (create, write, delete) could structure their filter section to look like the following (note the wildcard in the type field):

```
"Filters": [
    {
        "Type": "Event",
        "Data": {
            "Category": "File",
            "SubCategory": "",
            "Type": "*"
        }
    }
]
```

List of Responses

The following is a list of responses you can select and have the agent perform an action when the detection event is triggered.

Response	Description
Application Log	Logs detection events to the Windows Application Log
Delete Files	Permanently deletes any File Artifacts that are identified as an Artifact of Interest
Delete Registry Keys	Permanently deletes the entire Registry Key of any Artifacts of Interest that are identified as Registry Artifacts
Delete Registry Values	Permanently deletes the Registry Value of any Artifacts of Interest that are identified as Registry Artifacts
Log Off All Users	Logs off all users that are currently logged into the system
Log Off Inactive Users	Logs off all users that currently have an interactive session on the system
Log Off Remote Users	Logs off all users that currently have a remote session established on the system
Notification Window	Displays a Notification Window including the 'Detection Notification Message' utilizing the native Operating System notification box rather than the CylancePROTECT agent
Suspend Processes	Suspends any Process Artifacts that are identified as an Artifact of Interest
Suspend Process Tree	Suspends the entire process tree of any Process Artifacts that are identified as an Artifact of Interest The AOI is treated as the root of the tree.
Terminate Processes	Terminates any Process Artifacts that are identified as an Artifact of Interest
Terminate Process Tree	Terminates the entire process tree of any Process Artifacts that are identified as an Artifact of Interest The AOI is treated as the root of the tree.

Configurable Sensors

CylanceOPTICS version 2.4.2100 or later provides additional sensors to gather data. These sensors are enabled in a Device Policy, under the CylanceOPTICS settings.

Things to Know Before Enabling Sensors

- Enabling a sensor will increase the amount of data collected. This could impact the number of days worth of data saved in the local database.
- BlackBerry recommends testing a sensor on a small number of devices to assess the impact on data retention and device performance.

Enhanced Introspection Sensors

DNS Visibility

Signal to Noise Ratio	Potential Data Retention and Performance Impact	Recommended For	Not Recommended For
Moderate	Moderate	• Desktops • Laptops	• DNS Servers

Note:

- This sensor has the potential to gather a significant amount of data. However, it can provide visibility into data that other tools have difficulty recording.
- BlackBerry recommends that trusted tools that heavily rely on cloud-based services are whitelisted in CylanceOPTICS to allow for increased data retention.

Private Network Address Visibility

Signal to Noise Ratio	Potential Data Retention and Performance Impact	Recommended For	Not Recommended For
Low	High	• Desktops	• DNS Servers • Low or under resourced systems • Systems that are connected to via RDP or other remote access software.

Note:

- This sensor gathers a significant amount of data and will significantly impact the length of time that data is stored in the local database.
- BlackBerry recommends that this sensor only be enabled in environments where full visibility into private network address communication is an absolute requirement as many lateral movement techniques can be detected and prevented in other ways (such as by observing registry key changes, analyzing Powershell activity, etc.).

Windows Event Log Visibility

Signal to Noise Ratio	Potential Data Retention and Performance Impact	Recommended For	Not Recommended For
Moderate	Moderate	• Desktops • Laptops • Servers	• Domain Controllers • Exchange/Email Servers

Note:

- The Windows Event Logs that this sensor gathers data from will be generated frequently during normal system usage.
- Some organizations may already have tools in place that gather data from Windows Event Logs. BlackBerry recommends identifying if this data is already being collected using other mechanisms in an environment to reduce duplicate data, for increased data retention in CylanceOPTICS.

Advanced Scripting Visibility

Signal to Noise Ratio	Potential Data Retention and Performance Impact	Recommended For	Not Recommended For
High	Low to Moderate	• Desktops • Laptops • Servers	• Exchange/Email Servers

Note:

- Various tools provided by Microsoft or other third party security solutions may rely heavily on Powershell to conduct operations.
- BlackBerry recommends that trusted tools that heavily utilize Powershell are whitelisted in CylanceOPTICS to allow for increased data retention.

Advanced WMI Visibility

Signal to Noise Ratio	Potential Data Retention and Performance Impact	Recommended For	Not Recommended For
High	Low	• Desktops • Laptops • Servers	

Note:

- Some background and maintenance processes built into Windows operating systems utilize WMI to schedule tasks or execute commands which may result in bursts of high WMI activity on a system.
- BlackBerry recommends analyzing an environment for WMI usage prior to enabling this sensor.

Enhanced Portable Executable Parsing

Signal to Noise Ratio	Potential Data Retention and Performance Impact	Recommended For	Not Recommended For
Moderate	Low	• Desktops • Laptops • Servers	

Note:

- The data gathered by this sensor is only passed into the Context Analysis Engine to aid with advanced executable file analysis. It is not stored in the local database. This means that enabling this sensor will have little to no impact on data retention within CylanceOPTICS.

Enhanced Process and Hooking Visibility

Signal to Noise Ratio	Potential Data Retention and Performance Impact	Recommended For	Not Recommended For
Moderate	Low	• Desktops • Laptops • Servers	

Note:

- Some third-party security tools may utilize the Windows API's that this sensor gathers data from. In some cases, this will lead to irrelevant or trusted data being recorded by CylanceOPTICS.
- BlackBerry recommends that trusted security tools are whitelisted to allow for increased data retention and a higher Signal to Noise ratio.

Enhanced File Read Visibility

Signal to Noise Ratio	Potential Data Retention and Performance Impact	Recommended For	Not Recommended For
Moderate	Low	• Desktops • Laptops • Servers	

Note:

- Some third-party security tools may utilize the Windows API's that this sensor gathers data from. In some cases, this will lead to irrelevant or trusted data being recorded by CylanceOPTICS.
- BlackBerry recommends that trusted security tools are whitelisted to allow for increased data retention and a higher Signal to Noise ratio.

Sensed events, artifacts, and facets

Events, artifacts, and facets are the three primary data structuresloud that CylanceOPTICS uses to analyze, record, and investigate activities that occur on devices. A majority of CylanceOPTICS features rely on these data structures, including InstaQuery, Focus View, and Context Analysis Engine.

- You use InstaQuery to search devices for Indicators of Compromise (IOC's) by querying for a specific Artifact and Facet, like a File Path.
- You use Focus View to view the chain of Events leading up to a piece of malware being introduced to a device by showing a series of Events and each associated Artifact and Facet that make up the Event.
- CylanceOPTICS uses the Context Analysis Engine to inspect any number of Artifacts and Facets for every Event that occurs on a device, in near-real time.

The following information is an introduction and reference guide for understanding how CylanceOPTICS interprets and interacts with activities that are occurring on a device to better allow users to utilize Focus View, InstaQuery, and Context Analysis Engine.

Platform

The following is a list of data sources by operating system.

Platform	Data sources
Linux	ZeroMQ
macOS	CyOpticsDrvOSX kernel driver
Windows	CyOpticsDrv kernel driver Event tracking for Windows Security audit log

Events

Events are defined as the various components that lead to an observable change or action on a device. Events will always consist of two primary artifacts: the instigating artifact that initiates an action, and the target artifact that is being acted upon. Each of these artifacts may consist of secondary artifacts which are explained in a later section of this article.

CylanceOPTICS can sense five main categories of events that occur on a device:

- File
- Network
- Process
- Registry
- Thread

The tables below outlines these categories as well as their subcategories, types, and associated artifacts.

Event - Any

Policy option to enable: CylanceOPTICS ON

Event type	Description	Artifact type	Platform
Any	All events record the process that generated them, and the user associated with the action.	• Process • User	• Windows • macOS • Linux

Event - Application

Policy option to enable: Advanced WMI Visibility

Event type	Description	Artifact type	Platform
Create filter - consumer binding	A process used WMI persistence.	• WMI trace	• Windows
Create temporary consumer	A process is subscribing to WMI events.	• WMI trace	• Windows
Execute operation	A process performed a WMI operation.	• WMI trace	• Windows

Policy option to enable: Enhanced Process and Hooking Visibility

Event type	Description	Artifact type	Platform
CBT	SetWindowsHookEx API installed a hook to receive notifications useful to a CBT application.	• Windows event	• Windows
DebugProc	SetWindowsHookEx API installed a hook to debug other hook procedures.	• Windows event	• Windows
Get async key state	A process called the Win32 API GetAsyncKeyState	• Windows event	• Windows
JournalPlayback	SetWindowsHookEx API installed a hook to monitor posts messages previously recorded by a WH_JOURNALRECORD hook procedure.	• Windows event	• Windows

Event type	Description	Artifact type	Platform
JournalRecord	SetWindowsHookEx API installed a hook to monitor input messsages posted to the system message queue.	• Windows event	• Windows
Keyboard	SetWindowsHookEx installed a hook to monitor keystroke messages.	• Windows event	• Windows
LowLevel keyboard	SetWindowsHookEx API installed a hook to monitor low-level keyboard input events.	• Windows event	• Windows
LowLevel mouse	SetWindowsHookEx API installed a hook to monitor low-level mouse input events.	• Windows event	• Windows
Message	SetWindowsHookEx API installed a hook to monitor messages posted to a message queue.	• Windows event	• Windows
Mouse	SetWindowsHookEx API installed a hook to monitor mouse messages.	• Windows event	• Windows
Register raw input devices	A process called the Win32 API RegisterRawInputDevices.	• Windows event	• Windows
Set Windows event hook	A process called the Win32 API SetWinEventHook.	• Windows event	• Windows
Set Windows hook	SetWindowsHookEx installed an unlisted hook type value.	• Windows event	• Windows
ShellProc	SetWindowsHookEx API installed a hook to receive notifications useful to shell applications.	• Windows event	• Windows

Event type	Description	Artifact type	Platform
SysMsg	SetWindowsHookEx API installed a hook to monitor messages generated as a result of an input event in a dialog box, message box, or scroll bar.	- Windows event	- Windows
WindowProc	SetWindowsHookEx installed a hook to monitor Windows procedure messages.	- Windows event	- Windows

Event - Device

Policy option to enable: CylanceOPTICS ON

Event type	Description	Artifact type	Platform
Mount	Mount points often refer to a device being connected to a machine, but can also be folders mounted to specific network locations.	- File	- macOS - Linux

Event - File

Policy option to enable: CylanceOPTICS ON

Event type	Description	Artifact type	Platform
Create	A file was created.	- File	- Windows - macOS - Linux
Delete	A file was deleted.	- File	- Windows - macOS - Linux
Overwrite	A file was overwritten by another file.	- File	- Windows - macOS - Linux
Rename	A file was renamed.	- File	- Windows - macOS - Linux

Event type	Description	Artifact type	Platform
Write	A file was modified.	• File	• Windows • macOS • Linux

Policy option to enable: Enhanced File Read Visibility

Event type	Description	Artifact type	Platform
Open	A file was opened for reading.	• File	• Windows

Event - Memory

Policy option to enable: CylanceOPTICS ON

Event type	Description	Artifact type	Platform
Mmap	A region of memory has been mapped for a specific purpose, often due to being allocated for a process's use.	• Process	• macOS • Linux
MProtect	A region of memory has had its meta data changed, often to change its status, such as making it executable.	• Process	• macOS • Linux

Event - Network

Policy option to enable: CylanceOPTICS ON

Event type	Description	Artifact type	Platform
Connect	A network connection has been opened. By default, local traffic is not collected.	• Network	• Windows • macOS

Policy option to enable: Private Network Address Visibility

Event type	Description	Artifact type	Platform
Connect	Connect events include local traffic.	• Network	• Windows

Policy option to enable: DNS Visibility

Event type	Description	Artifact type	Platform
Request	A process made a non-cached, network DNS request.	- DNS request	- Windows
Response	A process received a DNS response.	- DNS request	- Windows

Event - Process

Policy option to enable: CylanceOPTICS ON

Event type	Description	Artifact type	Platform
Abnormal exit	Monitored by the preselect sensor, a process has exited without reaching its done state. This includes things like an exception causing the process to exit.	- Process	- macOS - Linux
Exit	A process has exited	- Process	- Windows - macOS - Linux
Forced exit	Monitored by the preselect sensor, a process has been forced to exit by another process.	- Process	- macOS - Linux
PTrace	A Unix system tool that allows one process to monitor and control another process.	- Process	- macOS - Linux
Start	A process has started.	- Process	- Windows - macOS - Linux
Suspend	Monitored by the preselect sensor, a process has been suspended.	- Process	- Linux

Event type	Description	Artifact type	Platform
Unknown Linux process event	Monitored by the preselect sensor, an unknown event has occurred with the process as a target, this can be any number of things, but shouldn't happen. If it does, it could be a sign of malicious software masking its activity.	• Process	• macOS • Linux

Policy option to enable: Enhanced Process and Hooking Visibility

Event type	Description	Artifact type	Platform
SetThreadContext	A process called the SetThreadContext Windows API.	• Process	• Windows
Terminate	An instigating process terminated another target process.	• Process	• Windows

Event - Registry

Policy option to enable: CylanceOPTICS ON

Event type	Description	Artifact type	Platform
Key created	A registry key was created.	• Registry • File (if the registry key references a specific file)	• Windows
Key deleted	A registry key was deleted.	• Registry • File (if the registry key references a specific file)	• Windows
Value created	A new registry key has been created.	• Registry • File (if the registry key references a specific file)	• Windows

Event type	Description	Artifact type	Platform
Value deleted	An existing registry value was deleted.	- Registry - File (if the registry key references a specific file)	- Windows
Value modified	A registry key value has been changed.	- Registry - File (if the registry key references a specific file)	- Windows

Event - Scripting

Policy option to enable: Advanced Scripting Visibility

Event type	Description	Artifact type	Platform
Execute command	Windows PowerShell executed a command, parameters unknown.	- File - Powershell trace	- Windows
Execute script	Antimalware Scan Interface (AMSI) ScanBuffer result indicated a script executed.	- File - Powershell trace	- Windows
Execute ScriptBlock	Windows PowerShell executed a script block.	- File - Powershell trace	- Windows
Invoke command	Windows PowerShell invoked a command with bound parameters.	- File - Powershell trace	- Windows
Prevent script	Antimalware Scan Interface (AMSI) ScanBuffer result indicated a script was blocked by an admin or detected.	- Powershell trace	- Windows

Event - User

Policy option to enable: Advanced Scripting Visibility

Event type	Description	Artifact type	Platform
Batch logoff	Batch logoff to Event ID 4634, type 4.	- Windows event	- Windows

Event type	Description	Artifact type	Platform
Batch logon	Batch logon corresponds to Windows Event ID 4624, type 4 - Scheduled task.	• Windows event	• Windows
CacheInteractive logoff	CacheInteractive logoff corresponds to Windows Event ID 4634, type 11.	• Windows event	• Windows
CacheInteractive logon	CacheInteractive logon corresponds to Windows Event ID 4624, type 11 - Logon with cached domain credentials such as when logging on to a laptop when away from the network.	• Windows event	• Windows
Interactive logoff	Interactive logoff corresponds to Windows Event ID 4634, type 2.	• Windows event	• Windows
Interactive logon	Interactive logon corresponds to Windows Event ID 4624, type 2 - Logon at keyboard and screen of system.	• Windows event	• Windows
Network logoff	Network logoff corresponds to Windows Event ID 4634, type 3.	• Windows event	• Windows
Network logon	Network logon corresponds to Windows Event ID 4624, type 3 - Connection to shared folder on this computer from elsewhere on network.	• Windows event	• Windows
NetworkClearText logoff	Corresponds to Windows Event ID 4634, type 8.	• Windows event	• Windows

Event type	Description	Artifact type	Platform
NetworkClearText logon	NetworkClearText logoff corresponds to Windows Event ID 4624, type 8 - Logon with credentials sent in clear text. Most often indicates a logon to IIS with basic authentication.	- Windows event	- Windows
NewCredentials logoff	NewCredentials logoff corresponds to Windows Event ID 4634, type 9.	- Windows event	- Windows
NewCredentials logon	NewCredentials logon corresponds to Windows Event ID 4624, type 9 - Example: RunAs or mapping a network drive with alternate credentials.	- Windows event	- Windows
RemoteInteraction logoff	RemoteInteraction logoff corresponds to Windows Event ID 4634, type 10.	- Windows event	- Windows
RemoteInteraction logon	RemoteInteraction logon corresponds to Windows Event ID 4624, type 10 - Terminal Services, Remote Desktop, or Remote Assistance.	- Windows event	- Windows
Service logoff	Service logoff corresponds to Windows Event ID 4634, type 5.	- Windows event	- Windows
Service logon	Service logon corresponds to Windows Event ID 4624, type 5 - Service startup.	- Windows event	- Windows
Unlock logoff	Unlock logoff corresponds to Windows Event ID 4634, type 7.	- Windows event	- Windows

Event type	Description	Artifact type	Platform
Unlock logon	Unlock logon corresponds to Windows Event ID 4624, type 7 - Unattended workstation with password protected screen saver.	• Windows event	• Windows
User logoff	User logoff corresponds to Windows Event ID 4634 with an unlisted type value.	• Windows event	• Windows
User logon	User logon corresponds to Windows Event ID 4624 with an unlisted type value.	• Windows event	• Windows

Artifacts and facets

Artifacts are complex pieces of information that can be used within CylanceOPTICS. The Context Analysis Engine utilizes artifacts of interest (AOI) as specifically tagged artifacts that automated response actions can be applied to for automatic incident response and incident remediation while InstaQuery utilizes artifacts as the foundation of a query. CylanceOPTICS uses six artifacts:

- File
- Network connections
- Processes
- Registry key
- Threads
- Users

Facets are attributes of artifacts that can be used to identify traits or qualities of an Artifact that is associated with an event. Facets can be logically combined during analysis for further conviction of maliciousness or suspiciousness. For example, a file named "explorer.exe" may not be inherently suspicious; however, if a file that is named "explorer.exe" is not signed by Microsoft, and resizes in a temporary directory, it may be deemed as suspicious in some environments. The table below outlines the Artifacts and their associated Facets that are currently supported by CylanceOPTICS.

Artifact	Facets
DNS	• Connection • IsRecursionDesired • IsUnsolicitedResponse • Opcode • RequestId • Resolution • ResponseOriginatedFromThisDevice • Questions

Artifact	Facets
Event	• Occurrence time (time the operating system recorded the event, if available) • Registration time (time CylanceOPTICS processed the event)
File	• Executable file record (binaries only) • File creation time (OS-reported) • File path • File signature (binaries only) • File size • Last modified time (OS-reported) • md5 hash (binaries only) • Recent write location • sha256 hash (binaries only) • Suspected file type • User
Network	• Local address • Local port • Protocol (example: UDP/TCP) • Remote address • Remote port
Powershell trace	• EventId • Payload • PayloadAnalysis • ScriptBlockText • ScriptBlockTextAnalysis
Process	• Command line • File the executable was run from • Parent process • Process ID • Start time • User
Registry	• If the value references a file on the system • Registry path • Value

Artifact	Facets
Users	• Domain • OS-specific identifier (example: SID) • User name User artifacts can also potentially contain any of the following values. However, on most endpoints, the data is not available. • AccountType • BadPasswordCount • Comment • CountryCode • FullName • HasPasswordExpired • HomeDirectory • IsAccountDisabled • IsLocalAccount • IsLockedOut • IsPasswordRequired • LanguageCodePage • LogonServer • PasswordAge • PasswordDoesNotExpire • ProfilePath • ScriptPath • UserPrivilege • Workstations
Windows event	• Class • Event ID • Provider
WMI trace	• ConsumerText • ConsumerTextAnalysis • EventId • Namespace • Operation • OperationAnalysis • OriginatingMachineName

Legal notice

This documentation including all documentation incorporated by reference herein such as documentation provided or made available on the BlackBerry website provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by BlackBerry Limited and its affiliated companies ("BlackBerry") and BlackBerry assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect BlackBerry proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of BlackBerry technology in generalized terms. BlackBerry reserves the right to periodically change information that is contained in this documentation; however, BlackBerry makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.

This documentation might contain references to third-party sources of information, hardware or software, products or services including components and content such as content protected by copyright and/or third-party websites (collectively the "Third Party Products and Services"). BlackBerry does not control, and is not responsible for, any Third Party Products and Services including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third Party Products and Services. The inclusion of a reference to Third Party Products and Services in this documentation does not imply endorsement by BlackBerry of the Third Party Products and Services or the third party in any way.

EXCEPT TO THE EXTENT SPECIFICALLY PROHIBITED BY APPLICABLE LAW IN YOUR JURISDICTION, ALL CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, MERCHANTABLE QUALITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR TITLE, OR ARISING FROM A STATUTE OR CUSTOM OR A COURSE OF DEALING OR USAGE OF TRADE, OR RELATED TO THE DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN, ARE HEREBY EXCLUDED. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR PROVINCE. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES AND CONDITIONS. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES OR CONDITIONS RELATING TO THE DOCUMENTATION TO THE EXTENT THEY CANNOT BE EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE HEREBY LIMITED TO NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, IN NO EVENT SHALL BLACKBERRY BE LIABLE FOR ANY TYPE OF DAMAGES RELATED TO THIS DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH BLACKBERRY PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF BLACKBERRY PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES

WERE FORESEEN OR UNFORESEEN, AND EVEN IF BLACKBERRY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, BLACKBERRY SHALL HAVE NO OTHER OBLIGATION, DUTY, OR LIABILITY WHATSOEVER IN CONTRACT, TORT, OR OTHERWISE TO YOU INCLUDING ANY LIABILITY FOR NEGLIGENCE OR STRICT LIABILITY.

THE LIMITATIONS, EXCLUSIONS, AND DISCLAIMERS HEREIN SHALL APPLY: (A) IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND, OR ACTION BY YOU INCLUDING BUT NOT LIMITED TO BREACH OF CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND SHALL SURVIVE A FUNDAMENTAL BREACH OR BREACHES OR THE FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR OF ANY REMEDY CONTAINED HEREIN; AND (B) TO BLACKBERRY AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED BLACKBERRY DISTRIBUTORS (ALSO INCLUDING AIRTIME SERVICE PROVIDERS) AND THEIR RESPECTIVE DIRECTORS, EMPLOYEES, AND INDEPENDENT CONTRACTORS.

IN ADDITION TO THE LIMITATIONS AND EXCLUSIONS SET OUT ABOVE, IN NO EVENT SHALL ANY DIRECTOR, EMPLOYEE, AGENT, DISTRIBUTOR, SUPPLIER, INDEPENDENT CONTRACTOR OF BLACKBERRY OR ANY AFFILIATES OF BLACKBERRY HAVE ANY LIABILITY ARISING FROM OR RELATED TO THE DOCUMENTATION.

Prior to subscribing for, installing, or using any Third Party Products and Services, it is your responsibility to ensure that your airtime service provider has agreed to support all of their features. Some airtime service providers might not offer Internet browsing functionality with a subscription to the BlackBerry® Internet Service. Check with your service provider for availability, roaming arrangements, service plans and features. Installation or use of Third Party Products and Services with BlackBerry's products and services may require one or more patent, trademark, copyright, or other licenses in order to avoid infringement or violation of third party rights. You are solely responsible for determining whether to use Third Party Products and Services and if any third party licenses are required to do so. If required you are responsible for acquiring them. You should not install or use Third Party Products and Services until all necessary licenses have been acquired. Any Third Party Products and Services that are provided with BlackBerry's products and services are provided as a convenience to you and are provided "AS IS" with no express or implied conditions, endorsements, guarantees, representations, or warranties of any kind by BlackBerry and BlackBerry assumes no liability whatsoever, in relation thereto. Your use of Third Party Products and Services shall be governed by and subject to you agreeing to the terms of separate licenses and other agreements applicable thereto with third parties, except to the extent expressly covered by a license or other agreement with BlackBerry.

The terms of use of any BlackBerry product or service are set out in a separate license or other agreement with BlackBerry applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY EXPRESS WRITTEN AGREEMENTS OR WARRANTIES PROVIDED BY BLACKBERRY FOR PORTIONS OF ANY BLACKBERRY PRODUCT OR SERVICE OTHER THAN THIS DOCUMENTATION.

BlackBerry Enterprise Software incorporates certain third-party software. The license and copyright information associated with this software is available at http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp.

BlackBerry Limited
2200 University Avenue East
Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
Ground Floor, The Pearce Building, West Street,
Maidenhead, Berkshire SL6 1RL
United Kingdom

Published in Canada