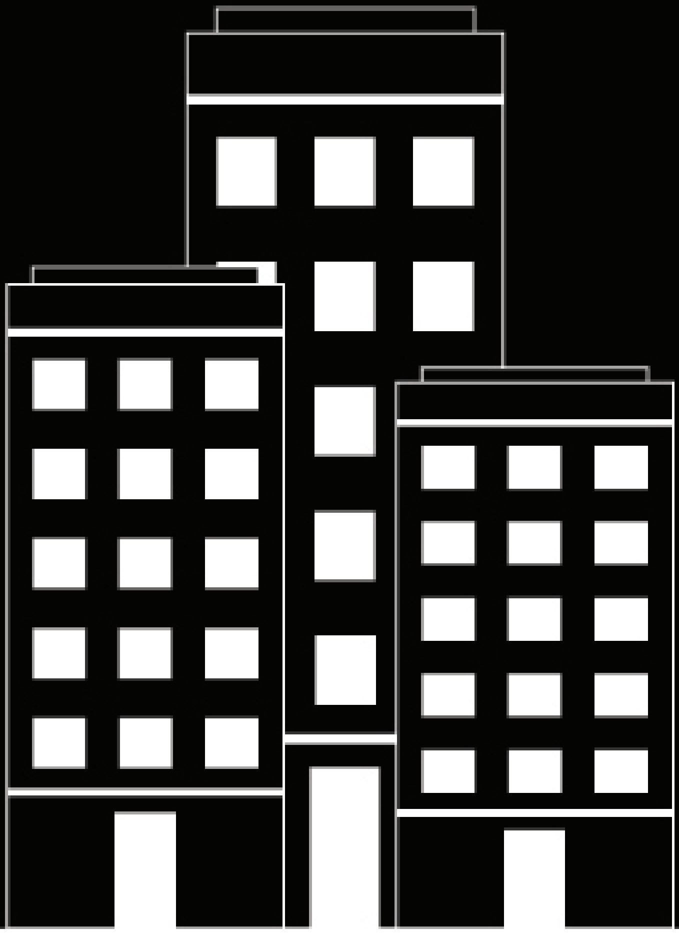


Cylance Endpoint Security

Administration Guide

Contents

Using dashboards

The dashboards offer helpful visualizations and statistical summaries of the data collected and analyzed by different Cylance Endpoint Security services. To view the dashboards, on the menu bar, click Dashboard and select the dashboard that you want to view. Default dashboards are available for CylancePROTECT Desktop, CylancePROTECT Mobile, and CylanceGATEWAY network data.

You can also create your own custom dashboards by selecting widgets that display the data collected by various services. Several widgets have interactive elements that you can manipulate to filter data or see more information, as well as links to view detailed information in dedicated screens in the management console.

You can share the dashboards that you create or modify with other administrator users.

Key features of Cylance Endpoint Security dashboards

Dashboard	Features
Device Protection (CylancePROTECT Desktop)	• Running Threats: View the count of threats that are currently running on devices. • Auto-Run Threats: View the count of threats that are set to run automatically. • Quarantined Threats: View the count of quarantined threats. • Unique to Cylance: View the count of threats that have been uniquely identified by CylancePROTECT Desktop. • Total Files Analyzed: View a count of the total number of files analyzed by CylancePROTECT Desktop. • Threat Events: View the threats detected over the last 30 days, classified by unsafe, abnormal, quarantined, waived, and cleared. • Threat Protection: View the percentage of threats on which you have taken action (for example, quarantine, waive, or added to the safe list). • Device Protection: View the percentage of devices with both unsafe and abnormal files configured for auto-quarantine in device policies. If auto-quarantine is disabled for one or both file types, the device is considered unprotected when calculating the percentage. • Threats By Priority: View the total number of threats, grouped by priority, that have not yet been acted on and require attention. • Threat Classifications: View a heat map of the types of threats detected. • Top Ten Lists: View the top ten threats found on the most devices, the top ten devices with the most threats, and the top ten zones with the most threats.

Dashboard	Features
Mobile Protection (CylancePROTECT Mobile)	• Mobile Alerts Detected: View the count of mobile alerts that are detected and the count of mobile alerts that are unresolved. • Mobile Devices with Alerts: View the count of mobile devices with alerts detected by the CylancePROTECT Mobile app. • Mobile Devices Enabled for Alerts Detection: View the count of mobile devices with the CylancePROTECT Mobile app installed and activated. • Mobile Alerts by Category: View charts and graphs of mobile alerts by category. • Mobile OSs with Vulnerabilities: View a graph of mobile operating systems with vulnerabilities, as identified, defined, and tracked by the National Vulnerability Database. • Mobile App Alerts: View statistics for detected malicious and sideloaded apps. • Mobile Network Alerts: View statistics for unsafe network and insecure Wi-Fi detections. • Mobile Device Security Alerts: View statistics for device security detections (screen lock disabled, attestation failure, and so on). • View lists and statistics for the top threats in the following categories: • Top Devices with Mobile Alerts • Top Insecure Wi-Fi Networks • Top Malicious Apps • Top Mobile Alert Detections • Top Sideloaded Apps • Top Unsafe Message URLs • Top Unsafe Networks • Top Unsupported Device Models • Top Unsupported OSs • Top Unsupported Security Patches

Dashboard	Features
Network (CylanceGATEWAY)	• Total Active Gateway Users: View the count of active users. • Network Connections: View a chart of allowed and blocked network connections. • Transferred Bytes: View a chart of transferred bytes (uploaded and downloaded). • Private Network Access, Public Network Access: View graphs of private and public network access. • Private Top Network Destinations, Public Top Network Destinations: View lists of the top private and public network destinations and top actions. • Connector Connection History: View a graph of online and offline CylanceGATEWAY Connectors. • Connector Status: View the connection status of the CylanceGATEWAY Connectors in your environment. • Destination Reputation Risk: View a list of low, medium, and high destination risk alerts. • Security Risk Categories: View the allowed, blocked, and combination of allowed and blocked risk categories for a specified category. • TLS Versions: View a chart of TLS versions in your environment. • Top Blocked Categories: View a graph of allowed, blocked, and combination of allowed and blocked destinations for the specified destination risk level. • Top Bandwidth Consumers: View a list of top bandwidth consumers in public, private, and combined public and private paths.
Information protection (CylanceAVERT)	• Information Exfiltration Events: View the count of CylanceAVERT exfiltration events, grouped by exfiltration type. This widget can be filtered by a custom time. • Top 10 Exfiltration Events by Category: View the count of the top 10 exfiltration events by category (policies, users, devices, files, and data types). This widget can be filtered by a custom time. • Top 10 File Inventory Items by Category: View the count of the top 10 inventory items by category (policies, file extensions, info types, and data types). • Top 10 Exfiltration Events by Location: View the count of the top 10 exfiltration events by location (web domains, email domains, and removable media). This widget can be filtered by a custom time. • File Inventory: View the count of sensitive files in the file inventory. • Evidence Locker: View the count of sensitive files in the evidence locker. • Total Active CylanceAVERT Users: View the count of total connected CylanceAVERT users. • Total Active CylanceAVERT Devices: View the count of total connected CylanceAVERT devices.

Create a dashboard

1. Do one of the following:

Task	Steps
Create a custom dashboard	**a.** In the management console, on the menu bar, click **Dashboard > Mobile Protection** or **Dashboard > Network**. **b.** Click ⊕ **> Add new dashboard**. **c.** If you want to start with a blank dashboard, in the drop-down list, click **New dashboard**. If you want the dashboard to have the default widgets for CylancePROTECT Mobile, CylanceGATEWAY (network), or CylanceAVERT (information protection), click that option in the drop-down list. **d.** Type a title. **e.** Click **Add**.
Copy a dashboard	**a.** In the management console, on the menu bar, click **Dashboard** and click the dashboard that you want to copy. **b.** Click ⊕ **> Copy this dashboard**. **c.** Type a title. **d.** Click **Save**.

2. Click ⊕ **> Add widgets**. For more information about the available widgets, see Key features of Cylance Endpoint Security dashboards.
3. From the **Add widgets** panel, drag and drop the widgets that you want to add to the dashboard.

   You can move widgets and resize them. To remove a widget, hover over it and click ⋮ **> Remove**.

Share a dashboard

You can share the dashboards that you create or modify with other administrator users.

Before you begin:

- You must have the Administrator role to share a dashboard with other administrators.
- Create a dashboard.

1. In the management console, navigate to the dashboard that you want to share.
2. Click ⋯ **> Share dashboard**.
3. Select whether you want to share the dashboard with all administrators or select administrators. If you choose to share with specific administrators, search for and add the administrators to the list.
4. Click **Share**.

The administrators that you shared the dashboard with will receive a notification when they log in to the management console. They can add the shared dashboard to their Dashboard menu by navigating to the default CylancePROTECT Mobile or CylanceGATEWAY dashboard, or any custom dashboard, clicking ⊕ **> Add new dashboard**, and selecting the shared dashboard in the new dashboard drop-down list. The users that you share a dashboard with cannot make changes to the shared dashboard, but they can copy it to create a new dashboard that they can modify.

The color of the icon next to the dashboard name indicates whether you are the owner of a shared dashboard (green), whether you have read-only access to a shared dashboard (brown), or whether the dashboard is shared with all administrators (orange).

After you finish:

- If you want to change who you share a dashboard with, navigate to the dashboard and click ⋯ **> Manage sharing settings**.
- If you want to stop sharing a dashboard, click ⋯ **> Stop sharing this dashboard**.

Managing alerts across Cylance Endpoint Security services

The Alerts view gives you a comprehensive way to review the alerts that are detected and correlated across Cylance Endpoint Security services, making it easier for you to identify and track prevailing threat patterns in your corporate ecosystem and resolve collections of alerts more efficiently. The Alerts view replaces the need to investigate alerts from various sections of the console that are each dedicated to a specific service such as CylancePROTECT Desktop or CylanceOPTICS. You can use the Alerts view to review, investigate, and manage alerts from any of the Cylance Endpoint Security services that your environment supports.

Service	Supported by the Alerts view
CylancePROTECT Desktop	Threat telemetry, memory protection alerts, and script control alerts from the CylancePROTECT Desktop agent on desktop devices.
CylancePROTECT Mobile	Alerts detected by the CylancePROTECT Mobile app.
CylanceOPTICS	Alerts detected by the CylanceOPTICS agent on desktop devices.
CylanceGATEWAY	Network protection settings that you have configured or the destination reputations that CylanceGATEWAY has determined to be high risk.
CylanceAVERT	Exfiltration events from the CylanceAVERT agent on desktop devices.
Okta connector	Okta user event telemetry using the BlackBerry Okta connector. Requires a CylanceENDPOINT Pro license.
Mimecast connector	Mimecast attachment protection telemetry using the BlackBerry Mimecast connector. Requires a CylanceENDPOINT Pro license.

The initial Alerts view is a summary that groups similar alerts based on criteria such as priority, alert classification, configured responses, and other key alert attributes. For more information about the criteria, see How Cylance Endpoint Security groups alerts.

The automated grouping of alerts reflects both the frequency and prevalence of alerts, giving analysts a clear view of how often threats occur and where they occur. By default, the alert groups are sorted in descending order by priority to provide a top-down view of all relevant security telemetry. Each group displays icons for the types of key indicator artifacts that are associated with the group (for example, File, Process, Email, and so on). You can click a key indicator icon to review the attributes of the key indicator, and, where applicable, you can copy or filter by those values. As new alerts are detected and processed from the telemetry sources, they are added to an existing group or to a new group.

The Alerts view supports single detection and multi-detection alerts. Alert detection rules can sometimes perform multiple detections before an alert is generated and displayed in the Alerts view. Each detection is modeled using an event (for example, File Opened, Registry Key Added, and so on).

You can click an alert group to access the following information:

- The alert overview tab that summarizes detection details and key indicators relevant to the group.
- The key indicators tab shows the detection attributes that are identical in each individual alert within the group. For example, if the key indicator was a file hash, that hash was detected in each alert, whether it was from the

same device or different devices. The key indicators are represented visually to show the relationship between parent, child, and sibling objects. For multi-detection alerts, the key indicators are included within each event and are summarized in the order of execution.
- The list of individual alerts in the group. You can click an individual alert to open granular details. You can also view the full set of artifacts, represented as icons, that are associated with the alert. The artifacts contain the full set of facets captured by the underlying detection engine. Like key indicators, these artifacts are represented visually to show the relationship between parent, child, and sibling objects. For multi-detection alerts, the key indicators are included within each event and are summarized in the order of execution.
- You can use the AI-powered Cylance Assistant to provide a summary analysis of an alert group, and detailed analysis for process artifacts within an alert group (for example, command line processes). The Cylance Assistant leverages rich cybersecurity knowledge sources to provide valuable information to aid you in your threat investigations. For more information, see Use the AI-powered Cylance Assistant to investigate alerts.

Depending on the types of alerts in a group, you may also be able to perform management actions. For example, for CylancePROTECT Desktop threat alerts, you can add a file to or remove a file from the global safe list or global quarantine list.

How Cylance Endpoint Security groups alerts

Cylance Endpoint Security uses the following criteria to group alerts from various services, automating the process to allow you to scope and optimize your threat-hunting and resolution activities to logical groupings of related alerts. The grouping logic is built and maintained by BlackBerry, and is dynamically designed to handle alerts from a range of integrated services. The result is a zero-touch experience that automates frequency and prevalence analysis, making it easier for you to triage and prioritize your cybersecurity efforts.

A new alert is added to an existing alert group when all of the following conditions are met:

- The priority, classification, sub-classification, description, key indicators, and response of the alert match that group.
- The alert is detected within 7 days (168 hours) of the oldest alert in that group.

A new alert group is created when an alert is detected that does not satisfy all of these conditions.

Priority

The priority of an alert, which correlates to the urgency of the issue and the potential impact on your organization’s environment, is factored into how alerts are grouped. The Alerts view groups the highest priority alerts across the telemetry sources to help you view and resolve the most important alerts first.

The factors that determine the priority of an alert vary by service:

Service	Factors
CylancePROTECT Desktop	• For threat alerts, the priority is always high in the Alerts view, even if the priority of the alert is lower in Protection > Threats in the management console. The purpose of this elevated priority in the Alerts view is to indicate the urgency of malware detections. • For memory protection and script control alerts, the priority is determined by the nature of the event, as configured by BlackBerry cybersecurity analysts. The priority is based on the overall severity and relevance for investigation.
CylancePROTECT Mobile	Alerts use a priority value that corresponds to the severity that is displayed in the management console and in the CylancePROTECT Mobile app.

Service	Factors
CylanceOPTICS	The priority is determined by the configuration of the CylanceOPTICS detection rules.
CylanceGATEWAY	Priority is based on the network protection settings that you configure or the reputation of a destination, as determined by CylanceGATEWAY, with a high risk level. For example, CylanceGATEWAY might generate alerts to display in the Alerts view in the following scenarios: • Destination reputation detections: • When enabled, the alerts are generated based on the risk level that you set. For example, if you set the risk level to "Medium and higher", alerts are generated for all the detections with the risk level of medium and high. • When not enabled, alerts that are determined to have a high risk level are generated by default. • Signature detections: • When enabled, alerts are generated for blocked signature detections and are displayed with a high risk level. • When not enabled, CylanceGATEWAY will not generate alerts. • For DNS Tunneling and Zero Day detections, alerts are generated for detections with a high risk level.
CylanceAVERT	The priority is always high in the Alerts view.
Mimecast	The priority is determined through Mimecast attachment risk scoring.
Okta	The priority is configured by BlackBerry cybersecurity analysts.

Classification and sub-classification

The alert classification and sub-classification identifies and labels the underlying detection type to provide structured alert content that can better describe the alert detected by a given service. Each service will define a specific set of classifications and sub-classifications to clarify the nature of the alert.

Classification and sub-classification data are used to identify and group similar alerts.

The factors that determine the classification and sub-classification of an alert vary by service:

Service	Factors
CylancePROTECT Desktop	• For threat alerts, the classification and sub-classification correspond to the file classifications for CylancePROTECT Desktop threat alerts. • For memory protection alerts, the classification and sub-classification correspond to the memory protection violation types. • For script control alerts, the classification indicates the overall alert type (for example, Script Control, Potentially Unwanted Program, Malware) and the sub-classification provides further detail (for example, Script Executed, Script Blocked).

Service	Factors
CylancePROTECT Mobile	The classification corresponds to an overall category of alerts (for example, Device Security or Network threats) and the sub-classification corresponds to the specific alert type that displays in the management console and in the app (for example, Malicious app, Sideloaded app, Insecure Wi-Fi, and so on).
CylanceOPTICS	Detection rules contain MITRE tactics, techniques, and sub-techniques to define the classification and sub-classification of an alert.
CylanceGATEWAY	The classification corresponds to the overall category of alerts (for example, Network Access Control) and the sub-classification corresponds to the specific alert type that displays in the management console (for example, Reputation, DNS Tunneling, Signature detection, and Zero-Day detection).
CylanceAVERT	The classification is determined by the exfiltration event.
Mimecast	The classification of an alert is the Initial Access Mitre tactic (TA0001). The sub-classification for the same alert is the Phishing Mitre technique (T1566).
Okta	The classification of an alert is either user access control (for example, if the maximum sign in attempts are exceeded) or network access control (for example, if the IP request is blocked due to a blocklist rule). If the alert classification is user access control, the sub-classification will be user lockout. If the alert classification is network access control, the sub-classification will be IP address blocked.

Description

The description of an alert is a characteristic that provides a short segment of information about the alert. Alerts with matching descriptions are more likely to be grouped together.

Key indicators

Key indicators are the detection content that are common across every individual alert in an alert group. The aggregation process compares the key indicators of alerts to determine whether they should be grouped together. For example, if a file contains a key indicator SHA256 hash, the hash value is identical within each alert inside an alert group.

The key indicators of an alert vary by service:

Service	Factors
CylancePROTECT Desktop	• For threat alerts, the key indicator is the SHA256 hash. • For memory protection alerts, the key indicators are the unique characteristics of the event (for example, file data such as the SHA256 hash and the risk score). • For script control alerts, the key indicators are the unique characteristics of the event (for example, a file SHA256 hash, script type, and script name).

Service	Factors
CylancePROTECT Mobile	Key indicators correspond to the unique characteristics of a given mobile alert (for example, the package name of a sideloaded app, the SSID of an insecure Wi-Fi network, the model of an unsupported device, and so on).
CylanceOPTICS	Key indicators are the uniquely identifying facets of the artifacts that are associated with an alert. For example, for process artifacts, the key indicators are the following facets: SHA256 hash, file path, and command line argument. These facets establish a unique signature for the process artifact type that can be compared to other alerts. The key indicator facets for an alert group are common across the individual alerts in the group.
CylanceGATEWAY	The key indicators are "Network connection" and "DNS request".
CylanceAVERT	The key indicators vary by the artifact type. For email alert artifacts, the key indicator is the conversationID. For browser and file exfiltration alert artifacts, the key indicator is the UserName.
Mimecast	The key indicators are the facets of the artifacts that are associated with an alert. For example, for email attachment artifacts, the key indicators are the SHA256 hash of the email file attachment.
Okta	The key indicators are the accounts associated with user login requests and the IP address associated with blocked login attempts.

Response

For services that execute mitigation actions, this is the action that you configured the service to execute in response to the detection. For example, for CylancePROTECT Desktop threat alerts, a response may be one of the following: waived, quarantined, unsafe, or abnormal.

For services that don't execute mitigation actions, this captures relevant information from the integrated service. Alerts with matching responses are more likely to be grouped together.

Time

The time that an alert occurs relative to other alerts is factored into how alerts are grouped. An alert is added to an existing group if the priority, classification, sub-classification, description, key indicators, and response of the alert match that group, and the alert occurs within 7 days (168 hours) of the oldest alert in that group. If the alert matches the above criteria but occurs outside of the 7 day window from the oldest alert in the group, it is added to a new group. The 7 day window ensures that alert groups have a fixed period and do not grow indefinitely.

View and manage aggregated alerts

Before you begin: Verify that your administrator role has the permissions required to use the Alerts view. The View alerts permission provides read-only access to the Alerts view. You require the Edit alerts and Delete alerts permissions to make changes to alert groups and individual alerts in this view. If you want to use the Alerts view to add a file from CylancePROTECT Desktop threat alerts to the global safe list or global quarantine list, or to remove a file from these lists, your role requires the associated global list permissions. For more information, see Setting up administrators in the Setup content.

1. In the management console, on the menu bar, click **Alerts**.

   To select the columns that you want to display, scroll to the right and click |||.
2. Do any of the following:

Task	Steps
Filter and sort alert groups.	**a.** Click ☰ on a column and type or select the filter criteria. You can do any of the following: • Apply multiple filter criteria at once. To remove a filter, click x for that filter. • If you want to filter by Classification, Sub-classification, Description, or Key Indicators, do one of the following: • To find exact matches, click ⚙ > **is equal to**. Type a value to view matches. Click up to 5 matches to add to the filtering list, then click **Apply**. • To find matches that contain the specified value, click ⚙ > **contains**. Type one or more values (click + to add additional values). Click **Apply**. When you view the results, you can click the filter displayed at the top of the screen to add or remove filter criteria. • If you filter by **Count**, click ⚙ for additional options (greater than, less than, and so on). • Filter by **Product** to scope results to specific Cylance Endpoint Security services. • Filter by **Detection Time** to scope results to a specific date and time range. **b.** To sort the alert groups in ascending or descending order by a column, click the name of the column (where applicable).
View details for key indicators of an alert group and filter alert groups by key indicator type or value.	**a.** Hover over a key indicator icon to see the type of object or event. Click an icon to view details. **b.** Where applicable, to view the full text of a truncated string value, hover over it and click ⛶. **c.** Where applicable, to copy a value, hover over it and click ⎘. **d.** To filter alert groups by key indicator, hover over it and click ☰.

Task	Steps
View details for an alert group and individual alerts.	**a.** Click an alert group. **b.** In the left pane, scroll down to view relationships between instigating and target objects. This view will show a single set of key indicators associated with individual events (files, users, executables, processes, and so on). **c.** In the left pane, scroll down to view relationships between instigating and target objects. This view will show a single set of key indicators associated with individual events (files, users, executables, processes, and so on). For example, you may see a parent process object or executable file that is the instigating process for a child process. Events or objects at the same level are considered siblings under the same parent. Where applicable, you can hover over values and click ⛶ to view full text strings or ⧉ to copy the value. For process artifacts, you can click 🛡 to generate an analysis by the Cylance Assistant. For more information, see Use the AI-powered Cylance Assistant to investigate alerts. **d.** For the individual device alerts, do any of the following: • Sort and filter the alert information. • Change the status of the alerts. See Status changes for alerts. • Assign the alerts to a user. • Add or change labels for the alerts. **e.** To open the details panel for an individual alert, click the alert. Do any of the following: • If applicable, you can click **Detection Detail** to view further details and actions in other areas of the console (for example, in the CylanceOPTICS detections view). The Detection Detail link will remain active for 60 days for CylancePROTECT Desktop threat alerts and for 30 days for other types of alerts. • Expand the artifacts associated with the alert to review details and view relationships between instigating and target objects and events. The complete set of objects associated with a detection rule are included in the artifacts view. Where applicable, you can hover over values and click ⛶ to view full text strings or ⧉ to copy the value. For process artifacts, you can click 🛡 to generate an analysis by the Cylance Assistant. For more information, see Use the AI-powered Cylance Assistant to investigate alerts.

Task	Steps
CylancePROTECT Desktop threat alerts: Add a file to or remove a file from the global safe list or global quarantine list.	**a.** Click an alert group that contains CylancePROTECT Desktop threat alerts. **b.** Click **Actions > Manage global list**. The SHA256 hash of the file associated with the threat alerts is displayed. A notification is provided if the file already exists in the global safe list or global quarantine list. **c.** Select the appropriate action to add the file to or remove the file from the global safe list or global quarantine list. If the file already exists in the global safe list or global quarantine list, you can move it to the other list. **d.** If you are adding the file to the global safe list, in the **Category** drop-down list, click the appropriate category. **e.** If you are adding the file to a list, type the reason. **f.** Click **Save**. The changes are applied to the appropriate safe or quarantine list. There is no change to the alert group in the Alerts view.
Change the status of alert groups.	Do any of the following: • To change the status of an alert group, in the **Status** drop-down list, click the appropriate status. • To change the status of multiple alert groups, select the alert groups, click **Change Status**, click the appropriate status, and click **Apply**. See Status changes for alerts.
Assign alert groups to a user.	Do any of the following: • To assign an alert group to a user, in the **Assignee** column, click +, search for and click a user, and click **Assign**. • To assign multiple alert groups to a user, select the alert groups, click **Assign Alert**, search for and select a user, and click **Assign**.
Add or change the label for alert groups.	You can add custom labels to alert groups to provide short notes or reminders or to use as filter criteria. To view labels you must set the Labels column to display. **a.** Select one or more alert groups. **b.** Click **Change Labels**. **c.** Type a label and press ENTER or search for and select an existing label. **d.** Click **Apply**. To remove a label, click the label, click the x icon, and click **Apply**.
Export alert data.	Do any of the following: • To export details for all alert groups, click ⍈. Specify the file name and type and click **Export**. • To export details for all of the alerts within a group, click an alert group, then click ⍈. Specify the file name and type and click **Export**.

Task	Steps
Delete alert groups.	**a.** Select one or more alert groups. **b.** Click **Delete**. **c.** Click **Delete** again to confirm.
Delete alert groups from filter results	**a.** Filter alert groups by the appropriate criteria. **b.** Do one of the following: • To delete all alert groups from the filter results, select the top-left check box and click **Delete All**. Click **Delete All** again to confirm. • To delete specific alert groups from the filter results, select the alert groups and click **Delete**. Click **Delete** again to confirm.

Use the AI-powered Cylance Assistant to investigate alerts

You can use the AI-powered Cylance Assistant to provide a summary analysis of an alert group, and detailed analysis for process artifacts within an alert group (for example, command line processes). The Cylance Assistant leverages rich cybersecurity knowledge sources to provide valuable information to aid you in your threat investigations.

Note:

- To access the Cylance Assistant in the Alerts view, you must contact your BlackBerry account representative to request enablement of this feature.
- Currently, the Cylance Assistant is available for CylanceOPTICS alerts only. Future updates will extend this functionality to other Cylance products and services.
- BlackBerry does not use any customer data to train the AI that powers the Cylance Assistant.

1. In the management console, on the menu bar, click **Alerts**.
2. On the **Product** column, click ⏷ and select **CylanceOPTICS**.
3. Click an alert group.

Task	Steps
Generate a summary analysis of the alert group.	**a.** In the left pane, in the **Overview** section, click **Alert Summary**. **b.** Click 📄 to copy the summary.
Generate an analysis of an instigating or target process for the alert group.	**a.** In the left pane, scroll down to view relationships between instigating and target objects. **b.** Hover over an instigating or target process artifact and click 🛡. **c.** Click 📄 to copy the analysis.
Generate an analysis of an instigating or target process for a specific alert in the group.	**a.** Click an individual alert in the alert group. **b.** In the right pane, scroll down to view relationships between instigating and target objects. **c.** Hover over an instigating or target process artifact and click 🛡. **d.** Click 📄 to copy the analysis.

Status changes for alerts

The status of individual alerts in other sections of the console (for example, Protection > Threats, CylanceOPTICS > Detections, and Protection > Protect Mobile alerts) correspond to an equivalent status in the Alerts view. When an alert status changes in another view, the status is also updated in the Alerts view. For example, if the status of an alert in Detections changes to False Positive, the status in the Alerts view changes to Closed.

When you change the status of individual alerts in the Alerts view, an equivalent status change is displayed in the CylanceOPTICS > Detections view. Currently, status changes that you initiate in the Alerts view will not be displayed in the Protection > Threats view or in the Protection > Protect Mobile alerts view.

Note the following equivalent states for CylancePROTECT Desktop threat alerts:

- Alerts displayed in Protection > Threats with an Unsafe, Abnormal, or Quarantined status have a New status in the Alerts view.
- Alerts displayed in Protection > Threats with a Waived status have a Closed status in the Alerts view.

If you set a status for an alert group, the individual alerts in that group are assigned the status that you selected. If the individual alerts in an alert group have different statuses, either from manual status changes or as a result of status changes that come from another view (for example, CylanceOPTICS > Detections), the status of the alert group changes to Multiple. If all of the individual alerts in an alert group have the same status, the alert group will also have the same status. For example, if all of the individual alerts have a status of Closed, the status of the alert group is also Closed.

Managing users, devices, and groups

This section provides information about how to view and manage the users and devices that are enabled for Cylance Endpoint Security services and the groups that you use to apply settings and policies.

Manage CylancePROTECT Desktop and CylanceOPTICS devices

You can use the management console to view and manage devices with the CylancePROTECT Desktop agent and the CylanceOPTICS agent from the **Assets > Devices** screen. Devices appear on this screen if they have successfully installed the agent and therefore registered with the management console. You can search for devices, export a device report, and perform actions on them. For example, you might want to export a list of devices that are running unsupported agents. Or, you can quickly add devices to another zone to ensure they are assigned an appropriate device policy according to their zone.

1. In the management console, on the menu bar, click **Assets > Devices**.
   A list of all devices is displayed.
2. Optionally, customize the columns displayed in the device grid.
   - To add or remove columns, click ||| and select the columns that you want displayed.
   - To rearrange the order of the columns, drag the column names to the position that you want.
   - To sort by ascending or descending order, click the name of a column.
3. To perform actions on devices, do any of the following:

Task	Steps
View device details.	Click a device name.
Assign a device policy to devices.	A device can be associated with one device policy only. If you assign a new device policy to a device, it replaces the previous device policy. **a.** Select one or more devices. **b.** Click **Assign Policy**. **c.** Click a device policy. **d.** Click **Save**.
Add devices to a zone.	You can use zones to manage the application of settings and a device policy to multiple devices. For more information about zones, see the Cylance Endpoint Security Setup content. **a.** Select one or more devices. **b.** Click **Add to Zones**. **c.** Select one or more zones. **d.** Click **Save**.

Task	Steps
Remove devices.	When you remove a device, you unregister the CylancePROTECT Desktop agent and the data for that device is removed from the management console. The user receives a notification that the agent is not registered and they need to provide an installation token to register the agent again. **a.** Select one or more devices. **b.** Click **Remove**. **c.** Click **Yes** to confirm.
Include (or exclude) devices in lifecycle management.	You can configure lifecycle management settings to specify when the state of a device changes from offline to inactive. For more information, see Using device lifecycle management. **a.** Select one or more devices. **b.** Click **Include In Lifecycle Management** or **Exclude From Lifecycle Management**. **c.** Click **Yes** to confirm.
Reset the inactivity period for devices.	This feature sets the device state to offline, resets the offline date counter, and sets the offline date to the current date. This does not affect devices that are online. **a.** Select one or more devices. **b.** Click **Reset inactivity period**. **c.** Click **Yes** to confirm.
Start a background threat detection scan on a device	You can start a background threat detection scan for a device on demand. This feature requires devices to be running CylancePROTECT Desktop agent version 3.2 or later. When you start a background scan with this option, any scan that is currently in progress on a device is terminated before the new scan is started. **a.** Select one or more devices. **b.** Click **Background scan**. **c.** Click **Yes** to confirm. The date and time that the most recent background scan completed is logged in the console. If recurring background threat detection is set in the assigned device policy, the next scheduled scan time is recalculated accordingly. Note that if background threat detection scans are running on several VM devices that are from the same VM host at the same time, device performance will be impacted due to resource sharing.

Manage zones

You can use zones to group and manage CylancePROTECT Desktop devices and CylanceOPTICS devices. You can group devices based on geography (for example, Asia and Europe), function (for example, Sales and IT staff), or by any criteria that your organization requires.

You can assign a device policy to a zone and apply that device policy to the CylancePROTECT Desktop and CylanceOPTICS devices that belong to that zone. You can also add a zone rule that can assign devices to a zone based on selected criteria, like domain name, IP address range, or operating system. A zone rule will add new devices to the zone if the device meets the rule requirements.

1. In the management console, on the menu bar, click **Zones**. Do any of the following:
    - To sort zones in ascending or descending order by a column, click the name of the column.
    - To filter the zones, click ≡ on a column and type or select the filter criteria.
2. Do any of the following:

Task	Steps
View the details for a zone.	Click a zone name.
Add a new zone.	**a.** Click **Add New Zone**. **b.** In the **Zone Name** field, type a name for the zone. **c.** In the **Policy** drop-down list, click a device policy to associate with the zone. **d.** In the **Value** field, click the appropriate priority level for the zone. This setting has no impact on managing zones. **e.** Click **Save**.
Remove a zone.	**a.** Select one or more zones. **b.** Click **Remove**. **c.** Click **Yes**.
Create a zone rule.	Create a zone rule to automatically add devices to a zone if they meet specified criteria. The rule conditions that you specify are processed in order from top to bottom. **a.** Click a zone name. **b.** Click **Create Rule**. **c.** Configure the zone rule. **d.** Click **Save**.
Add devices to a zone.	The maximum number of zones a device can belong to is 75. If a device has over 75 zones, there may be unexpected results with the policy and agent assignment or an error message indicating "Failed to add selected Devices to selected Zones." **a.** Click a zone name. **b.** On the **Devices** tab, click **Add Device to Zone**. **c.** Select the devices that you want to add. **d.** If you want to apply the zone device policy to those devices, select the **Apply zone policy to selected devices** check box. **e.** Click **Save**.

Task	Steps
Apply the zone device policy to all users in the zone.	This action replaces any device policies that are currently assigned to devices with the device policy that is currently assigned to the zone. **a.** Click a zone name. **b.** Select the **Apply to all devices in this zone** check box. **c.** Click **Save**.
Copy devices to another zone.	**a.** Click a zone name. **b.** On the **Devices** tab, select one or more devices. **c.** Click **Copy Device**. **d.** Select one or more zones. **e.** Click **Save**.
Remove devices from the zone.	**a.** Click a zone name. **b.** On the **Devices** tab, select one or more devices. **c.** Click **Remove Device from Zone**. **d.** Click **Yes**.
Use zones to manage agent updates.	You can create zone-based update rules to update the CylancePROTECT Desktop and CylanceOPTICS agents on devices. For more information, see the Cylance Endpoint Security Setup content.

Manage devices with the CylancePROTECT Mobile app

You can use the management console to view and manage mobile devices with the CylancePROTECT Mobile app. You can also view the current risk level of devices, which is determined using the mapping of threats to risk levels in the risk assessment policy that is assigned to users (there is a default assessment policy). For more information about risk assessment policies, see the Cylance Endpoint Security Setup content.

1. In the management console, on the menu bar, click **Assets > Mobile Devices**. Do any of the following:
   - To sort devices in ascending or descending order by a column, click the name of the column.
   - To filter the devices, click ≡ on a column and type or select the filter criteria.
2. Do any of the following:

Task	Steps
View the CylancePROTECT Mobile alerts for a device.	**a.** Click a device. **b.** View the **Protect Mobile Alerts** tab. To view the alerts that resulted in the device's current risk level, in the left pane, click the risk level.
View the CylanceGATEWAY events for a device.	**a.** Click a device. **b.** On the menu, click **Events**.
View the compliance details for a device.	**a.** Click a device. **b.** On the menu, click **Compliance**.

Task	Steps
Delete devices.	**a.** Select one or more devices. **b.** Click **Remove**. **c.** Click **Remove** again to confirm. The device and all alerts and events associated with it are removed from the Cylance Endpoint Security services and management console. If you want to add the device again, the user must reactivate the CylancePROTECT Mobile app. See Manage CylancePROTECT Mobile app and CylanceGATEWAY users for instructions for sending a new activation email.

Manage CylancePROTECT Mobile app and CylanceGATEWAY users

You can view and manage user accounts that are enabled for the CylancePROTECT Mobile app and for CylanceGATEWAY in the management console.

1. In the management console, on the menu bar, click **Assets > Users**. Do any of the following:
    - To sort users in ascending or descending order by a column, click the name of the column.
    - To filter the users, click ≡ on a column and type or select the filter criteria.
2. Do any of the following:

Task	Steps
View a user's alerts.	**a.** Click a user's name. **b.** On the menu, click **Alerts**. **c.** Click the appropriate tab.
View a user's events.	**a.** Click a user's name. **b.** On the menu, click **Events**.
View a user's device details.	**a.** Click a user's name. **b.** On the menu, click **Devices**. **c.** Click a device to view the associated alerts, events, and compliance information.
Add a user to a group.	Directory groups are managed in your company directory, so you can't use the steps below to add users to directory groups. These steps apply to local groups only. **a.** Click a user's name. **b.** On the menu, click **Configuration**. **c.** Click **Assign User Groups**. **d.** Search for and select one or more groups. **e.** Click **Assign**.

Task	Steps
Remove a user from a group.	Directory groups are managed in your company directory, so you can’t use the steps below to remove users from directory groups. These steps apply to local groups only. **a.** Click a user’s name. **b.** On the menu, click **Configuration**. **c.** Click 🗑 next to the group. **d.** Click **Unassign**.
Assign a policy to a user.	**a.** Click a user’s name. **b.** On the menu, click **Configuration**. **c.** Click **Assign User Policies**. **d.** In the policies drop-down list, click the type of policy. **e.** Search for and select the policy. **f.** Click **Assign**. If the user is already assigned a policy of that type, the new selection replaces the previously assigned policy.
Remove a policy from a user.	**a.** Click a user's name. **b.** On the menu, click **Configuration**. **c.** Click 🗑 next to the policy. **d.** Click **Unassign**.
Remove the One-Time Password enrollment from a user.	The user must be enrolled for One-Time Password. **a.** Click a user's name. **b.** In the **Actions** drop-down list, click **Remove TOTP enrollment**. **c.** In the **Remove TOTP enrollment** dialog box, click **Confirm**.
Send a new activation email for the CylancePROTECT Mobile app.	The user must be assigned an enrollment policy with the applicable mobile platform enabled. **a.** Select one or more users. **b.** Click **Resend Invitation**. **c.** Click **Resend Invitation** again to confirm.
Expire a user’s activation password for the CylancePROTECT Mobile app.	**a.** Select one or more users. **b.** Click **Expire Passcode**. **c.** Click **Expire** to confirm.

Task	Steps
Delete users.	**a.** Select one or more users. **b.** Click **Delete Users**. **c.** Click **Delete** to confirm. The user account and all CylancePROTECT Mobile app and CylanceGATEWAY events and alerts associated with that user are removed from the Cylance Endpoint Security services and management console. If you configured directory synchronization and onboarding, modify the directory group as necessary so that the user is not added to Cylance Endpoint Security again when synchronization occurs.

View CylanceAVERT user details

You can view information about your CylanceAVERT users and associated events, devices, and policies from the **CylanceAVERT Users** page in the management console. When you select a user from the CylanceAVERT users list, you will be able to view the user's details, the data exfiltration events associated with that user, the device details for the user's devices, and the user groups and policies that the user is assigned to.

1. In the management console, on the menu bar, click **Assets > Avert Users**.
2. Click on a user's name from the Avert Users list to view a specific user's details. You can view each user's name, email address, and the number of devices assigned to the user from the Avert Users list.

   Note: You cannot add, update, or remove users from this page. If you would like to manage your users, click **Manage Users**.
3. From the user details page, do any of the following:
   - To view details about the data exfiltration events associated with the user, click the **Events** tab. This tab displays by default.
   - To view details about the users devices, including the device name, OS version, CylanceAVERT agent version, the agent enrollment date, and the time that the last policy was assigned, click the **Devices** tab.
   - To view the user groups and user policies assigned to the user, click the **Configuration** tab. To assign the user to user groups, click **Assign User Groups**, then select the group from the list. To assign the user to a user policy, click **Assign User Policies**, then select the policy from the drop-down menu.

Manage user groups

You can manage user groups for users who are enabled for the CylancePROTECT Mobile app and for CylanceGATEWAY users. A user group is a collection of related users who share common properties. Administering users as a group is more efficient than administering individual users because properties can be added, changed, or removed for all members of the group at the same time. When you assign policies to user groups, the policies apply to all members of the group.

Cylance Endpoint Security has two types of user groups:

- Directory groups link to groups in your company directory. The membership of the group synchronizes with the membership list in the directory. For more information, see Configure onboarding and offboarding.
- Local groups are created and maintained in the management console. You can assign any local user or directory user to a local group.

For more information about creating groups, see the Setup content.

1. In the management console, on the menu bar, click **Assets > User Groups**.
2. To assign policies to the group, under policies, click ⊕ and select the policy that you want to assign.

   You can also assign policies to users and groups from the policy settings.
3. To manage users in the group, click the **Users** tab.

Configure device lifecycle management

Agents have the offline status when they are not communicating with the management console, such as when the user turns off their device. If an agent remains in the offline state for a long period of time, this could indicate that the device is no longer being used.

Using device lifecycle management, you can specify the number of days that a device can remain offline before it is marked as inactive in the management console. When a device is marked as inactive, you have the option to automatically remove it from the console after another specified number of days. For example, you can configure the device lifecycle management feature to mark an offline device as inactive after it has remained offline for 30 days. You can also configure the feature to remove a device from the console after it has been inactive for another 15 days.

When the device lifecycle management feature is enabled or changed, the system checks the offline date of each offline device and updates their status within 24 hours. For example, if there is a device that has been offline for 40 days, and the device lifecycle management feature is enabled and the Days Offline field is set to 30 days, the device state will change to "inactive" within a 24 hours. In another example, if there is a device that has been offline for 25 days, and the Days Offline field is set to 30 days, the device state will be set to "inactive" in 5 days, assuming it remains offline.

The console tracks the number of days that the device has remained in the offline or inactive states. When the device communicates with the console again, the device state changes to online and the timer resets.

1. In the management console, click **Settings > Device Lifecycle**.
2. Turn on the **Enable automated device lifecycle management** setting.
   a) In the **Days Offline** field, specify the number of days (7 to 180) that a device must be offline before its status is changed to inactive.
3. To delete inactive devices, turn on the **Remove inactive devices** setting.
   a) In the **Days inactive** field, specify the number of days (7 to 180) that a device must be inactive before it is automatically removed from the console.

   When you remove a device from the console, the device's data is deleted from the console, but the agent is not deleted on the device.
4. Click **Save**.

After you finish:

- To view the state of a device, in **Assets > Devices**, see the **State** column.
- To view whether a device is included in device lifecycle management, in **Assets > Devices**, see the **Lifecycle management** column. If you don't see the column, you might need to manually reveal the column.
- To exclude a device from device lifecycle management so that it is not marked as inactive after being offline, see Manage CylancePROTECT Desktop and CylanceOPTICS devices.

View a list of applications installed on CylancePROTECT Desktop devices

The CylancePROTECT Desktop agent version 3.2 reports a list of software applications that are installed on the device to the console. This feature allows you to identify applications that are installed on devices that may be a source of vulnerabilities, prioritize actions against vulnerabilities, and manage them accordingly. You can view all applications that are installed on the devices and also view a list of applications that are installed on individual devices. This feature can be enabled from the device policy.

Before you begin:

- Devices must be running CylancePROTECT Desktop agent version 3.2 or later on a Windows device to report a list of applications to the console.
- Devices must be assigned a device policy with the software inventory feature turned on.

Do one of the following:

Task	Steps
View a list of all applications installed on devices in your tenant	**a.** In the console, go to **Assets > Installed Applications**. **b.** Click on an application name to view a list of devices that have it installed. You can click on a device name to view the device details, including a list of applications that are installed on the device.
View a list of applications installed on an individual device	**a.** In the console, go to **Assets > Devices**. **b.** Click on a device name. **c.** In the **Threats & activities** section, click the **Installed Applications** tab.

Remove a registered FIDO device for a user account

You can remove FIDO devices that a user has registered. For example, you can remove a registered device if it is lost or if the user has left your organization.

1. In the management console, on the menu bar, click **Assets > Users**.
2. n the **Actions** drop-down list, click **Manage FIDO devices**.
3. In the **Manage FIDO devices** dialog, select devices and click **Remove**.

Discover unprotected devices

You can use the management console to view a list of known devices, discovered from Active Directory, that are not protected by CylancePROTECT Desktop. Known devices that are running an OS version that supports the installation of CylancePROTECT are indicated. You can also export the device list and take necessary actions (for example, install CylancePROTECT) on those devices to protect those devices and your network from potential threats.

Before you begin: Ensure that you have enabled the Unprotected Device Discovery service. For more information, see Enable unprotected device discovery.

1. In the management console, on the menu bar, click **Assets > Unprotected Devices**.

The protection control status of the device can be any of the following:

- Supported: The discovered device is running an OS version that is supported by CylancePROTECT Desktop.
- Unsupported: The discovered device is not running an OS version that is supported by CylancePROTECT Desktop.
- Insufficient info: Not enough information is available to determine if the OS version that is running on the device is supported by CylancePROTECT Desktop.

2. Do any of the following:

   - To add or remove columns, click ||| and select the columns that you want to view.
   - To filter any of the columns, click in the column heading.
   - To export the unprotected devices to a .csv file, click ⇥. You can export all of the table columns or select **Current filters** to export only the filtered columns. Click **Export**.

Enable unprotected device discovery

You must enable the Unprotected Device Discovery service to scan the newly added tenant to detect and list known devices that are not protected by CylancePROTECT Desktop on the Unprotected Devices screen. The option to enable this service will be available within 24 hours after you have setup the directory connection with the BlackBerry Connectivity Node.

On newly added tenants, the option is unavailable for up to 24 hours while the service works on a scheduler that refreshes the tenant list and data from other services. This refresh occurs every 24 hours. After the tenant information is updated, the information is available to the Unprotect Device Discovery service and you can enable it. When the service is enabled for the first time, the unprotected devices will be listed within 2 minutes. After the service is enabled, the management console updates the unprotected devices list every 24 hours. By default, this feature is disabled for each tenant.

Before you begin:

- Ensure that you configured a directory connection using with the latest version of the BlackBerry Connectivity Node. For more information, see Installing the BlackBerry Connectivity Node in the Setup content.
- Configure your environment to view the device OS and OS version of managed unprotected devices.
- Make sure that the user has the appropriate permissions to enable this feature. For more information on permissions, see Permissions for administrator roles in the Setup content. The following permissions are required:
  - To view the Directory Connections, the user must have the 'View directory connections' permission.
  - To enable and disable this feature, the user must have the 'Edit directory connections' permission.

1. In the management console, on the menu bar, click **Settings > Directory Connections**.
2. In the **Directory Connection** list, click the connection that you want to enable unprotected device discovery for.
3. On the **Sync settings** tab, select **Unprotected Device Discovery**.
4. When you are prompted, click **Confirm** to apply this setting to all directory connections in your environment.

Configure your environment to view the device OS and OS version of managed unprotected devices

For the unprotected devices feature to display the device OS and OS version, you must configure the schema to allow the required attributes to synchronize from the domain controller to the Global Catalog.

1. On the Active Directory domain controller, complete the following steps to register Schmmgmt.dll and add the Schema option to the MMC:

   a) On the domain controller, click **Start > Run**.

   b) In the search field, type `regsvr32 schmmgmt.dll`. Click **OK**.

   c) When the operation completes, click **OK**.

2. In the MMC, open the Active Directory schema and do the following:
    a) Click **Start > Run**.
    b) In the search field, type `mmc.exe`. Click **OK**.
    c) On the **File** menu, click **Add/Remove Snap-in**.
    d) Click **Active Directory Schema**.
    e) Click **Add**.
    f) Click **Close**. Click **OK**.
3. To update the attributes to synchronize to the Global Catalog, do the following:
    a) In the left column of the Active Directory schema view, click **Attributes**.
    b) In the attributes list, search for and click **operatingSystem**.
    c) Select the **Replicate this attribute to the Global Catalog** checkbox.
    d) Click **OK**.
    e) Repeat steps a to d for the following attributes:

        - operatingSystemServicePack
        - operatingSystemVersion

Managing threats detected by CylancePROTECT Desktop

Devices are endpoints with the CylancePROTECT Desktop agent installed, for example, desktop computers or servers. Devices can be managed using the management console or the Cylance User API. Management actions include reviewing threat events and other alerts, verifying that the correct device policy and settings are assigned to devices, and using zones to group and simplify the management of devices.

Manage CylancePROTECT Desktop threat alerts

You can use the management console to view and manage threat alerts detected by the CylancePROTECT Desktop agent. Files that are considered unsafe or abnormal display in the management console. Files that are considered safe do not display in the console.

1. In the management console, on the menu bar, click **Protection > Threats**. Do any of the following:
    - To add or remove columns, click ⦀ and select the columns that you want to view.
    - To group the threat alert information by one or more columns, drag those columns to the space above the column names.
    - To sort threat alerts in ascending or descending order by a column, click the column.
    - To filter the threat alerts by a column, use the filter field and icon for the column. After you filter the threat alerts, save these filters by bookmarking the page. Saving your filters as a bookmark only works for threat alerts.
2. Do any of the following:

Task	Steps
View threat alert details.	Click on the threat alert row.
View the threat details page.	Click on the file name.
Use the threat filters.	Click a threat filter. Click the close icon to clear the threat filter.
View threat indicators.	Expand the **Threat indicators** section. For more information about threat indicators, see Threat indicators.
Add files to a global list.	Add files to the global quarantine or global safe list. **a.** Click the check boxes for the files to add to a global list. **b.** Click **Global quarantine** to add the files to the global quarantine list. Click **Safe** to add the files to the global safe list.
Add a file to a local list.	Add a file to a local quarantine or local safe list. Local lists take precedence over global lists. For example, you might want to block a file from the organization but allow it on specific devices. **a.** Click the threat alert row. **b.** On the devices list, under **Unsafe** or **Abnormal**, select the check boxes for the appropriate devices. **c.** Click **Quarantine** to add the file to the local quarantine list. Click **Waive** to add the file to the local safe list.

Task	Steps
Change the local list for a file.	You can change a file from the local quarantine to the local safe list or from the local safe list to the local quarantine. **a.** Click the threat alert row. **b.** On the devices list, under **Quarantined** or **Waived**, select the check boxes for the appropriate devices. **c.** If you are on the **Waived** list, click **Quarantine** to add the file to the local quarantine list. If you are on the **Quarantined** list, click **Waive** to add the file to the local safe list.

After you finish: To export the threat information to a .csv file, click ↗. Select the scope of the export and click **Export**.

Threat indicators

Each category represents an area that has been frequently seen in malicious software.

Anomalies

These indicators represent situations where the file has elements that are inconsistent or nomalous in some way. Frequently these are inconsistencies in structural elements in the file.

Indicator	Description
16bitSubsystem	The file utilizes the 16-bit subsystem. Malware uses this to exist in a less secure and less monitored part of the operating system, and frequently to perform privilege escalation attacks.
Anachronism	This PE appears to be lying about when it was written, which is atypical for professionally written software.
AppendedData	This PE has some extra content appended to it, beyond the normal areas of the file. Appended data can frequently be used to embed malicious code or data, and is frequently overlooked by protection systems.
AutoitDbgPrivilege	The AutoIt script is capable of performing debug activities.
AutoitManyDllCalls	The AutoIt script uses many external DLL calls. The AutoIt runtime already has many common functions, therefore using additional functionality from external DLLs may be a sign of maliciousness.
AutoitMutex	The AutoIt script creates synchronization objects. This is often used by malware to prevent multiple infections of the same target.
AutoitProcessCarving	The AutoIt script is likely performing process carving to run its own code that appears to come from another process. This is often done to hinder detection.
AutoitProcessInjection	The AutoIt script is likely performing process injection to run code in other processes' context possibly to stay undetected or to steal data.

Indicator	Description
AutoitRegWrite	The AutoIt script writes into the Windows registry.
Base64Alphabet	The file contains evidence of usage of Base64 encoding of an alphabet. Malware does this to attempt to avoid common detection, or to attack other programs using Base64 encoding.
CommandlineArgsImport	The file imports functions that can be used to read arguments from a command line. Malware uses this to collect information on subsequent runs.
ComplexMultipleFilters	The file contains multiple streams with multiple filters.
ComplexObfuscatedEncoding	The file contains an anomalously high number of obfuscated names.
ComplexUnsupportedVersion EmbeddedFiles	The file uses EmbeddedFiles features from newer versions of the PDF standard than the file declares.
ComplexUnsupportedVersionFlate	The file uses the FlateDecode feature from newer versions of the PDF standard than the file declares.
ComplexUnsupportedVersionJbig2	The file uses the JBIG2Decode feature from newer versions of the PDF standard than the file declares.
ComplexUnsupportedVersionJs	The file uses JavaScript features from newer versions of the PDF standard than the file declares.
ComplexUnsupportedVersionXFA	The file uses XFA features from newer versions of the PDF standard than the file declares.
ComplexUnsupportedVersionXobject	The file uses XOBject features from newer versions of the PDF standard than the file declares.
ContainsFlash	The file contains flash objects.
ContainsPE	The file contains embedded executable files.
ContainsU3D	The file contains U3D objects.
InvalidCodePageUsed	The file uses an invalid or unrecognized locale, possibly to avoid detection.
InvalidData	The file metadata is obviously bogus or corrupt.
InvalidStructure	The file structure is not valid. The sizes, metadata, or internal sector allocation table is wrong, which may indicate an exploit.
ManifestMismatch	The file demonstrates an inconsistency in its manifest. Malware does this to avoid detection, but rarely covers its tracks deeply.

Indicator	Description
NontrivialDLLEP	This PE is a DLL with a nontrivial entry point. This is common among DLLs, but a malicious DLL may use its entry point to take up residence in a process.
NullValuesInStrings	Some strings within the file contain null characters in the middle.
PDFParserArraysContainsNullCount	The file contains an anomalously high number of null values in arrays.
PDFParserArraysHeterogeneousCount	The file contains an anomalously high number of arrays containing different types of elements.
PDFParserMailtoURICount	The file contains an anomalously high number of email links (mailto:).
PDFParserMinPageCount	The file has an unusual structure of page objects, such as a high number of child-page objects per node.
PDFParserNamesPoundNameMaxLength	The file may attempt to obfuscate its contents by using long encoded strings.
PDFParserNamesPoundNameMinLength	The file contains an anomalously high minimum length of an escaped name.
PDFParserNamesPoundNameTotalLength	The file may attempt to obfuscate its contents by storing much of its content in encoded strings.
PDFParserNamesPoundNameUpperCount	The file contains an anomalously high number of names escaped with uppercase hexadecimal characters.
PDFParserNamesPoundNameValidCount	The file contains an anomalously high number of valid escaped names.
PDFParserNamesPoundPerNameMaxCount	The file contains an anomalously high maximum number of escaped characters per single name.
PDFParserNamesPoundUnnecessaryCount	The file contains an anomalously high number of unnecessarily escaped names.
PDFParserNumbersLeadingDigitTallies8	The file contains an anomalously high number of numbers that start with 8 in decimal representation.
PDFParserNumbersPlusCount	The file contains an anomalously high number of numbers with explicit plus sign.
PDFParserNumbersRealMaxRawLength	The file contains an anomalously high maximum length of a real number.

Indicator	Description
PDFParserPageCounts	The file contains an anomalously high number of child-page objects.
PDFParserPageObjectCount	The file contains an anomalously high number of page objects.
PDFParserSizeEOF	The file contains an anomalously long end-of-file sequence(s).
PDFParserStringsHexLowerCount	The file contains an anomalously high number of strings escaped with lowercase hexadecimal digits.
PDFParserStringsLiteralString MaxLength	The file contains an anomalously high maximum length of a literal string.
PDFParserStringsOctalZero PaddedCount	The file contains an anomalously high number of octal escaped characters in strings that are unnecessarily zero-padded.
PDFParserTrailerSpread	The file contains an anomalously large spread between trailer objects.
PDFParserWhitespaceComment MaxLength	The file contains an anomalously high maximum length for a comment.
PDFParserWhitespaceComment MinLength	The file contains unusual short comments that are not used by reader software.
PDFParserWhitespaceComment TotalLength	The file contains an unusually large amount of commented-out data.
PDFParserWhitespaceEOL0ACount	The file contains an anomalously high number of short end-of-line characters.
PDFParserWhitespaceWhitespace 00Count	The file contains an anomalously high number of zero-bytes used as whitespace.
PDFParserWhitespaceWhitespace 09Count	The file contains an anomalously high number of 09 bytes used as whitespace.
PDFParserWhitespaceWhitespace LongestRun	The file contains an anomalously long whitespace area.
PDFParserWhitespaceWhitespace TotalLength	The file contains an anomalously high number of whitespaces.
PDFParseru3DObjectsNames AllNames	The file contains an anomalously high number of U3D objects.

Indicator	Description
PossibleBAT	The file contains evidence of having a standard Windows batch file included. Malware does this to avoid common scanning techniques and to provide persistence.
PossibleDinkumware	The file shows evidence of including some components from DinkumWare. Dinkumware is frequently used in various malware components.
PropertyImpropriety	The file contains suspicious OOXML properties.
RaiseExceptionImports	The file imports functions used to raise exceptions within a program. Malware does this to implement tactics that make standard dynamic code analysis difficult to follow.
ReservedFieldsViolation	The file violates the specification in terms of the use of reserved fields.
ResourceAnomaly	The file contains an anomaly in the resource section. Malware frequently contains malformed or other odd bits in the resource section of a DLL.
RWXSection	This PE may contain modifiable code, which is at best unorthodox and at worst symptomatic of a virus infection. Frequently, this feature implies that the file has been built using something other than a standard compiler, or has been modified after it was originally built.
SectorMalfeasance	The file contains structural oddities with OLE sector allocation.
StringInvalid	One of the references to a string in a string table pointed to a negative offset.
StringTableNotTerminated	A string table was not terminated with a null byte. This could cause a fault at runtime due to a string that does not end.
StringTruncated	One of the references to a string in a string table pointed to a location after the end of a file.
SuspiciousPDataSection	This PE is hiding something in its "pdata" area, but it is not clear what it is. The "pdata" area in a PE file is generally used for process runtime structures, but this particular file contains something else.
SuspiciousRelocSection	This PE is hiding something in its "relocations" area, but it is not clear what it is. The "relocations" area in a PE file is generally used for relocating particular symbols, but this particular file contains something else.
SuspiciousDirectoryNames	The file contains OLE directory names associated with badness.
SuspiciousDirectoryStructure	The file has oddities in the OLE directory structure.
SuspiciousEmbedding	The file uses suspicious embedding of OLE.

Indicator	Description
SuspiciousVBA	The file contains suspicious VBA code.
SuspiciousVBALib	The file shows suspicious VBA library usage.
SuspiciousVBANames	The file contains suspicious names associated with VBA structures.
SuspiciousVBAVersion	The file contains suspicious VBA versioning.
SWFOddity	The file contains certain questionable usages of embedded SWF.
TooMalformedToProcess	The file is so malformed that it could not be parsed completely.
VersionAnomaly	The file has issues with how it presents its version information. Malware does this to avoid detection.

Collection

These indicators represent situations where the file has elements that indicate capabilities or evidence of collecting data. This can include the enumeration of system configuration or collection of specific sensitive information.

Indicator	Description
BrowserInfoTheft	The file contains evidence of an intent to read passwords stored in browser caches. Malware uses this to collect the passwords for exfiltration.
CredentialProvider	The file contains evidence of interaction with a credential provider, or the desire to appear as one. Malware does this because credential providers get access to many types of sensitive data, such as usernames and passwords, and by acting as one, they may be able to subvert the authentication integrity.
CurrentUserInfoImports	The file imports functions that are used to gather information about the currently logged-in user. Malware uses this to determine paths of action to escalate privileges and to better tailor attacks.
DebugStringImports	The file imports functions that are used to output debug strings. Typically, this is disabled in production software, but left on in malware that is being tested.
DiskInfoImports	The file imports functions that can be used to gather details about volumes on the system. Malware uses this in conjunction with listing to determine facts about the volumes in preparation for a further attack.
EnumerateFileImports	The file imports functions that are used to list files. Malware uses this to look for sensitive data, or to find further points of attack.
EnumerateModuleImports	The file imports functions that can be used to list all of the DLLs that a running process uses. Malware uses this capability to locate and target specific libraries for loading into a process, and to map out a process it wishes to inject into.

Indicator	Description
EnumerateNetwork	The file demonstrates evidence of a capability to attempt to enumerate connected networks and network adapters. Malware will do this to determine where a target system lies in relation to others, and to look for possible lateral paths.
EnumerateProcessImports	The file imports functions that can be used to list all of the running processes on a system. Malware used this capability to locate processes to inject into or those that it wishes to delete.
EnumerateVolumeImports	The file imports functions that can be used to list the volumes on the system. Malware uses this to find all of the areas it might need to search for data, or to spread an infection.
GinaImports	The file imports functions that are used to access Gina. Malware does this to attempt to breach the secure ctrl-alt-delete password entry system or other network login functions.
HostnameSearchImports	The file imports functions that are used to gather information about host names on the network and the host name of the machine itself. Malware uses this capability to better target further attacks or scan for new targets.
KeystrokeLogImports	The file imports functions that can capture and log keystrokes from the keyboard. Malware uses this to capture and save keystrokes to find sensitive information such as passwords.
OSInfoImports	The file imports functions that are used to gather information about the current operating system. Malware uses this to determine how to better tailor further attacks and to report information back to a controller.
PossibleKeylogger	The file contains evidence of key-logger type activity. Malware uses keyloggers to collect sensitive information from the keyboard.
PossiblePasswords	The file has evidence of including common passwords, or a structure that would enable brute forcing common passwords. Malware uses this to attempt to penetrate a network further by accessing other resources via password.
ProcessorInfoWMI	The file imports functions that can be used to determine details about the processor. Malware uses this to tailor attacks and exfiltrate this data to common command-and-control infrastructure.
RDPUsage	The file shows evidence of interacting with the Remote Desktop Protocol (RDP). Malware frequently uses this to move laterally and to offer direct command-and-control functionality.
SpyString	The file is possibly spying on the clipboard or user actions via accessibility API usage.
SystemDirImports	The file imports functions used to locate the system directory. Malware does this to find where many of the installed system binaries are located, as it frequently hides among them.

Indicator	Description
UserEnvInfoImports	The file imports functions that are used to gather information about the environment of the current logged-in user. Malware uses this to determine details about the logged-in user and look for other intelligence that can be gleaned from the environment variables.

Data loss

These indicators represent situations where the file has elements that indicate capabilities or evidence of exfiltration of data. This can include outgoing network connections, evidence of acting as a browser, or other network communications.

Indicator	Description
AbnormalNetworkActivity	The file implements a non-standard method of networking. Malware does this to avoid detection of more common networking approaches.
BrowserPluginString	The file has the capability to enumerate or install browser plugins.
ContainsBrowserString	The file contains evidence of attempting to create a custom UserAgent string. Malware frequently uses common UserAgent strings to avoid detection in outgoing requests.
DownloadFileImports	The file imports functions that can be used to download files to the system. Malware uses this as both a way to further stage an attack and to exfiltrate data via the outbound URL.
FirewallModifyImports	The file imports functions used to modify the local Windows firewall. Malware uses this to open holes and avoid detection.
HTTPCustomHeaders	The file contains evidence of the creation of other custom HTTP headers. Malware does this to facilitate interactions with command-and-control infrastructures and to avoid detection.
IRCCommands	The file contains evidence of interaction with an IRC server. Malware commonly uses IRC to facilitate a command-and-control infrastructure.
MemoryExfiltrationImports	The file imports functions that can be used to read memory from a running process. Malware uses this to determine proper places to insert itself, or to extract useful information from the memory of a running process, such as passwords, credit cards, or other sensitive information.
NetworkOutboundImports	The file imports functions that can be used to send data out to the network or the general Internet. Malware uses this as a method for exfiltration of data or as a method for command and control.
PipeUsage	The file imports functions that allow the manipulation of named pipes. Malware uses this as a method of communication and of data exfiltration.

Indicator	Description
RPCUsage	The file imports functions that allow it to interact with Remote Procedure Call (RPC) infrastructure. Malware uses this to spread, or to send data to remote systems for exfiltration.

Deception

These indicators represent situations where the file has elements that indicate capabilities or evidence of a file attempting to be deceptive. Deception can come in the form of hidden sections, inclusion of code to avoid detection, or indications that it is labeled improperly in metadata or other sections.

Indicator	Description
AddedHeader	The file contains an additional, obfuscated PE header that may be a hidden malicious payload.
AddedKernel32	The file contains an additional, obfuscated reference to kernel32.dll, a library that may be used by malicious payload.
AddedMscoree	The file contains an additional, obfuscated reference to mscoree.dll, a library that may be used by malicious payload.
AddedMsvbvm	The file contains an additional, obfuscated reference to msvbvm, a library that may be used by malicious payload compiled for Microsoft Visual Basic 6.
AntiVM	The file demonstrates features that can be used to determine if the process is running in a virtual machine. Malware does this to avoid running in virtualized sandboxes that are becoming more common.
AutoitDownloadExecute	The AutoIt script can download and execute files. This is often done to deliver additional malicious payloads.
AutoitObfuscationStringConcat	The AutoIt script is likely obfuscated with string concatenation. This is often done to avoid detection of whole, suspicious commands.
AutoitShellcodeCalling	The AutoIt script uses the CallWindowProc() Windows API function that may indicate the injection of shellcode.
AutoitUseResources	The AutoIt script uses data from resources stored alongside the script. Malware often stores important parts of itself as resource data and unpacks them in runtime, and therefore this looks suspicious.
CabinentUsage	The file shows evidence of containing a CAB file. Malware does this to package sensitive components in a way that many detection systems cannot see.
ClearKernel32	The file contains a reference to kernel32.dll, a library that may be used by a malicious payload.

Indicator	Description
ClearMscoree	The file contains a reference to mscoree.dll, a library that may be used by a malicious payload.
ClearMsvbvm	The file contains a reference to msvbvm.dll, a library that may be used by malicious payload compiled for Microsoft Visual Basic 6.
ComplexInvalidVersion	The file declares the wrong PDF version.
ComplexJsStenographySuspected	The file may contain JavaScript code hidden in literal strings.
ContainsEmbeddedDocument	The file contains a document embedded inside the object. Malware can use this to spread an attack to multiple sources or to otherwise hide its true form.
CryptoKeys	The file contains evidence of having an embedded cryptographic key. Malware does this to avoid detection and perhaps as authentication with remote services.
DebugCheckImports	The file imports functions that would allow it to act like a debugger. Malware uses this capability to read and write from other processes.
EmbeddedPE	The PE has additional PEs within it, which is usually only the case with software installation programs. Frequently malware embeds a PE file that it then drops to disk and executes. This technique is often used to avoid protection scanners by packaging binaries in a format that the underlying scanning technology does not understand.
EncodedDosStub1	The PE contains an obfuscated PE DOS stub that may belong to a hidden malicious payload.
EncodedDosStub2	The PE contains an obfuscated PE DOS stub that may belong to a hidden malicious payload.
EncodedPE	The PE has additional PEs hidden within it, which is extremely suspicious. It is similar to the EmbeddedPE indicator, but uses an encoding scheme to attempt to further hide the binary inside the object.
ExecuteDLL	The PE contains evidence of the capability to execute a DLL using common methods. Malware does this as a method to avoid common detection practices.
FakeMicrosoft	The PE claims to be written by Microsoft, but it does not look like a Microsoft PE. Malware commonly masquerades as Microsoft PEs in order to look inconspicuous.
HiddenMachO	The file has another MachO executable file within, which is not properly declared. This may be an attempt to hide the payload from being easily detected.

Indicator	Description
HTTPCustomUserAgent	The file contains evidence of manipulation of the browser UserAgent. Malware does this to facilitate interactions with command-and-control and to avoid detection.
InjectProcessImports	The PE can inject code into other processes. This capability frequently implies that a process is attempting to be deceptive or hostile in some way.
InvisibleEXE	The PE appears to run invisibly, but it is not a background service. It might be designed to remain hidden.
JSTokensSuspicious	The file contains unusually suspicious JavaScript.
MSCertStore	The file shows evidence of interacting with the core Windows certificate store. Malware does this to collect credentials and to insert rogue keys into the stream to facilitate actions such as man-in-the-middle attacks.
MSCryptoImports	The file imports functions to use the core Windows cryptography library. Malware will use this to leverage the locally installed cryptography so it does not need to carry around its own cryptography.
PDFParserDotDotSlash1URICount	The file may attempt path traversal using relative paths such as "../".
PDFParserJavaScriptMagicseval~28	The file may contain obfuscated JavaScript or can run dynamically loaded JavaScript with eval().
PDFParserJavaScriptMagic sunescape~28	The file may contain obfuscated JavaScript.
PDFParserjsObjectsLength	The file contains an anomalously high number of individual JavaScript scripts.
PDFParserJSStreamCount	The file contains an unusually high number of JavaScript-related streams.
PDFParserJSTokenCounts0 cumulativesum	The file contains an anomalously high number of JavaScript tokens.
PDFParserJSTokenCounts1 cumulativesum	The file contains an anomalously high number of JavaScript tokens.
PDFParserNamesAllNames Suspicious	The file contains an anomalously high number of suspicious names.
PDFParserNamesObfuscatedNames Suspicious	The file contains an anomalously high number of obfuscated names.
PDFParserPEDetections	The file contains embedded PE file(s).

Indicator	Description
PDFParserSwfObjectsxObservations SWFObjectsversion	The file contains an SWF object with an unusual version number.
PDFParserSwfObjectsxObservation sxSWFObjectsxZLibcmfSWFObjectsx ZLibcmf	The file contains an SWF object with unusual compression parameters.
PDFParserswfObjectsxObservations xSWFObjectsxZLibflg	The file contains an SWF object with unusual compression flag parameters.
PE_ClearDosStub1	The file contains a DOS stub, indicative of PE file inclusion.
PE_ClearDosStub2	The file contains a DOS stub, indicative of PE file inclusion.
PE_ClearHeader	The file contains PE file header data that does not belong in the file structure.
PEinAppendedSpace	The file contains a PE file that does not belong in the file structure.
PEinFreeSpace	The file contains a PE file that does not belong in the file structure.
ProtectionExamination	The file seems to be looking for common protection systems. Malware does this to initiate an anti-protection action tailored to that installed on the system.
SegmentSuspiciousName	A segment has either an invalid string as a name or an unusual non-standard name. This may indicate post-compilation tampering or use of packers or obfuscators.
SegmentSuspiciousSize	The segment size is significantly different from the size of all content sections within. This may indicate the use of an unreferenced area or the reservation of space for runtime unpacking of malicious code.
SelfExtraction	The file seems to be a self-extracting archive. Malware frequently uses this tactic to obfuscate their true intentions.
ServiceDLL	The file seems to be a service DLL. Service DLL's are loaded in the svchost.exe process and are a common persistence methodology for malware.
StringJsSplitting	The file contains suspicious JS tokens.
SWFinAppendedSpace	The file contains a Shockwave flash object that does not belong in the document structure.
TempFileImports	The file imports functions used to access and manipulate temporary files. Malware does this because temporary files tend to avoid detection.

Indicator	Description
UsesCompression	The file seems to have portions of the code that appear to be compressed. Malware uses these techniques to avoid detection.
VirtualProtectImports	The file imports functions that are used to modify the memory of a running process. Malware does this to inject itself into running processes.
XoredHeader	The file contains an xor-obfuscated PE header that may be a hidden malicious payload.
XoredKernel32	The file contains an xor-obfuscated reference to kernel32.dll, a library that may be used by a malicious payload.
XoredMscoree	The file contains an xor-obfuscated reference to mscoree.dll, a library that may be used by a malicious payload.
XoredMsvbvm	The file contains an xor-obfuscated reference to msvbvm.dll, a library that may be used by a malicious payload compiled for Microsoft Visual Basic 6.

Destruction

These indicators represent situations where the file has elements that indicate capabilities or evidence of destruction. Destructive capabilities include the ability to delete system resources like files or directories.

Indicator	Description
action_writeByte	The VBA script within the document is likely writing bytes to a file, which is an unusual action for a legitimate document.
action_hexToBin	The VBA script within the file is likely using hexadecimal-to-binary conversion that may indicate decoding a hidden malicious payload.
appended_URI	The file contains a link that does not belong in the file structure.
appended_exploit	The file contains suspicious data outside of the file structure that may be indicative of an exploit.
appended_macro	The file contains a macro script that does not belong in the file structure.
appended_90_nopsled	The file contains a nop-sled that does not belong in the file structure; this is almost certainly there to facilitate exploitation.
AutorunsPersistence	The file attempts to interact with common methods of persistence (for example, startup scripts). Malware commonly uses these tactics to attain persistence.
DestructionString	The file has capabilities to kill processes or shut down the machine via shell commands.

Indicator	Description
FileDirDeleteImports	The PE imports functions that can be used to delete files or directories. Malware uses this to break systems and cover its tracks.
JsHeapSpray	The file likely contains heap spray code.
PossibleLocker	The file demonstrates evidence of a desire to lock out common tools by policy. Malware will do this to retain persistence and make detection and cleanup more difficult.
RegistryManipulation	The file imports functions that are used to manipulate the Windows registry. Malware does this to attain persistence, avoid detection, and for many other reasons.
SeBackupPrivilege	The PE might attempt to read files to which it has not been granted access. The SeBackup privilege allows access to files without honoring access controls. It is frequently used by programs that handle backups and is frequently limited to administrative users, but it can be used maliciously to gain access to specific elements that might otherwise be difficult to access.
SeDebugPrivilege	The PE might attempt to tamper with system processes. The SeDebug Privilege is used to access processes other than your own and is frequently limited to administrative users. It is often paired with reading and writing to other processes.
SeRestorePrivilege	The PE might attempt to change or delete files to which it has not been granted access. The SeRestore privilege allows writing without consideration of access control.
ServiceControlImports	The file imports functions that can control Windows services on the current system. Malware uses this either to launch itself into the background via installing as a service, or to disable other services that may have a protective function.
SkylinedHeapSpray	The file contains an unmodified version of skylined heap spray code.
SpawnProcessImports	The PE imports functions that can be used to spawn another process. Malware uses this to launch subsequent phases of an infection, typically downloaded from the Internet.
StringJsExploit	The file contains JavaScript code that is likely capable of exploitation.
StringJsObfuscation	The file contains JavaScript obfuscation tokens.
TerminateProcessImports	The file imports functions that can be used to stop a running process. Malware uses this to attempt to remove protection systems, or to cause damage to a running system.
trigger_AutoClose	The VBA script within the file is likely trying to execute automatically when the file is closing.

Indicator	Description
trigger_Auto_Close	The VBA script within the file is likely trying to execute automatically when the file is closing.
trigger_AutoExec	The VBA script within the file is likely trying to execute automatically.
trigger_AutoExit	The VBA script within the file is likely trying to execute automatically when the document is closing.
trigger_AutoNew	The VBA script within the file is likely trying to execute automatically when a new document is being created.
trigger_AutoOpen	The VBA script within the file is likely trying to execute as soon as the file is opened.
trigger_Auto_Open	The VBA script within the file is likely trying to execute as soon as the file is opened.
trigger_DocumentBeforeClose	The VBA script within the file is likely trying to execute automatically just before the file closes.
trigger_DocumentChange	The VBA script within the file is likely trying to execute automatically when the file is being changed.
trigger_Document_Close	The VBA script within the file is likely trying to execute automatically when the file is closing.
trigger_Document_New	The VBA script within the file is likely trying to execute automatically when a new file is being created.
trigger_DocumentOpen	The VBA script within the file is likely trying to execute as soon as the file is opened.
trigger_Document_Open	The VBA script within the file is likely trying to execute as soon as the file is opened.
trigger_NewDocument	The VBA script within the file is likely trying to execute automatically when a new file is being created.
trigger_Workbook_Close	The VBA script within the file is likely trying to execute automatically when a Microsoft Excel workbook is closing.
trigger_Workbook_Open	The VBA script within the file is likely trying to execute automatically when a Microsoft Excel workbook is opening.
UserManagementImports	The file imports functions that can be used to change users on the local system. It can add, delete, or change key user details. Malware can use this capability to achieve persistence or to cause harm to the local system.

Indicator	Description
VirtualAllocImports	The file imports functions that are used to create memory in a running process. Malware does this to inject itself into a running process.

Shellcodes

These indicators represent situations where a small piece of code is used as the payload in the exploitation of a software vulnerability. It is called shellcode because it typically starts a command shell from which the attacker can control the compromised machine, but any piece of code that performs a similar task can be called shellcode.

Indicator	Description
ApiHashing	The file contains a byte sequence that looks like shellcode that tries to stealthily find library APIs loaded in memory.
BlackholeV2	The file looks like it might have come from the Blackhole exploit kit.
ComplexGotoEmbed	The file may be able to force a browser to go to an address or perform an action.
ComplexSuspiciousHeader	The PDF header is located at a non-zero offset which may indicate an attempt to prevent this file from being recognized as a PDF document.
EmbeddedTiff	The file may contain a crafted TIFF image with nop-sled to facilitate exploitation.
EmbeddedXDP	The file likely contains another PDF as an XML Data Package (XDP).
FindKernel32Base1	The file contains a byte sequence that looks like a shellcode that tries to locate kernel32.dll in memory.
FindKernel32Base2	The file contains a byte sequence that looks like a shellcode that tries to locate kernel32.dll in memory.
FindKernel32Base3	The file contains a byte sequence that looks like a shellcode that tries to locate kernel32.dll in memory.
FunctionPrologSig	The file contains a byte sequence that is a typical function prolog, and likely contains shellcode.
GetEIP1	The file contains a byte sequence that looks like a shellcode that resolves its own address to locate other things in memory and facilitate exploitation.
GetEIP4	The file contains a byte sequence that looks like a shellcode that resolves its own address to locate other things in memory and facilitate exploitation.
IndirectFnCall1	The file contains a byte sequence that looks like an indirect function call, and is likely shellcode.
IndirectFnCall2	The file contains a byte sequence that looks like an indirect function call, and is likely shellcode.

Indicator	Description
IndirectFnCall3	The file contains a byte sequence that looks like an indirect function call, and is likely shellcode.
SehSig	The file contains a byte sequence that is typical for Structured Exception Handling (SEH), and likely contains shellcode.
StringLaunchActionBrowser	The file may be able to force a browser to go to an address or perform an action.
StringLaunchActionShell	The file may be able to execute shell actions.
StringSingExploit	The file might contain an exploit.

Miscellaneous indicators

This section lists the indicators that do not fit into the other categories.

Indicator	Description
AutoitFileOperations	The AutoIt script can perform multiple actions on files. This may be used for information gathering, persistence, or destruction.
AutorunString	The file has the capability to achieve persistence by using autorun mechanism(s).
CodepageLookupImports	The file imports functions used to look up the codepage (location) of a running system. Malware uses this to differentiate which country/region a system is running in to better target particular groups.
MutexImports	The file imports functions to create and manipulate mutex objects. Malware frequently uses mutexes to avoid infecting a system multiple times.
OpenSSLStatic	The file contains a version of OpenSSL compiled to appear stealthy. Malware does this to include cryptography functionality without leaving strong evidence of it.
PListString	The file has the capability to interact with property lists that are used by the operating system. This may be used to achieve persistence or to subvert various processes.
PrivEscalationCryptBase	The file shows evidence of attempting to use a privilege escalation using CryptBase. Malware uses this to gain more privileges on the affected system.
ShellCommandString	The file has the capability to use sensitive shell commands for reconnaissance, elevation of privilege, or data destruction.
SystemCallSuspicious	The file has the capability to monitor or control system and other processes, performing debug-like actions.

Manage CylancePROTECT Desktop script control alerts

You can use the management console to view and manage script control alerts detected by the CylancePROTECT Desktop agent. Scripts that are considered unsafe display in the management console.

1. In the management console, on the menu bar, click **Protection > Script Control**. Do any of the following:
    - To add or remove columns, click ||| and select the columns that you want to view.
    - To sort script control alerts in ascending or descending order by a column, click the column.
    - To filter the script control alerts by a column, use the filter field and icon for the column.
2. Do any of the following:

Task	Steps
View script control alert details.	**a.** Click on the script control alert row but not the check box. **b.** View the devices affected by the script control alert. A list of affected devices displays below the list of script control alerts.
Add a script to the global safe list.	Add a script to the global safe list. **a.** Click the check boxes for the scripts to add to a global list. **b.** Click **Safe**.
View the device details page.	**a.** Click on a device name to view the device details page.

After you finish: To export the script control information to a .csv file, click ↗. Select the scope of the export and click **Export**.

Manage CylancePROTECT Desktop external device alerts

You can use the management console to view and manage external device alerts detected by the CylancePROTECT Desktop agent. Examples of external devices include smartphones, flash drives, external hard drives, and digital cameras. External device settings are also known as device control.

Before you begin: Before you exclude an external device, consider the following:

- Adding an exclusion that contains underscores in the serial number is not supported from the external device alerts page. You must add the exclusion in the device policy.
- Adding an exclusion from the external device alerts page affects the policy currently assigned to the device, which might not be the policy used when the alert occurred.

1. In the management console, on the menu bar, click **Protection > External devices**. Do any of the following:
    - To add or remove columns, click ||| and select the columns that you want to view.
    - To group the external device alert information by one or more columns, drag those columns to the space above the column names.
    - To sort external device alerts in ascending or descending order by a column, click the column.
    - To filter the external device alerts by a column, use the filter field and icon for the column.
2. Do any of the following:

Task	Steps
Add the external device to the device policy exclusion list.	External device exclusions are configured in a device policy. Adding an exclusion from the external device alerts page adds the exclusion to the device policy assigned to the device the alert was detected on. **a.** Click ⊕ for the external device alert you want to add a device policy exclusion for. **b.** Optionally, you can change the product ID and serial number for the external device. The vendor ID cannot be changed. **c.** Optionally, you can add a comment. You can provide a reason for the exclusion or other relevant information. **d.** Select one of the following access types: • Full access: Allows the external device to connect to the endpoint and provides full access to the external device (read and write access). • Read only: Allows the external device to connect to the endpoint but provides read-only access to the external device. • Block: Does not allow the external device to connect to the endpoint. **e.** Click **Save exclusion**.
View the device details page.	**a.** Click on a device name to view the device details page.

After you finish: To export the external device information to a .csv file, click ↗. Select the scope of the export and click **Export**.

Threat protection

CylancePROTECT Desktop can do more than simply classify files as unsafe or abnormal. It can provide details on the static and dynamic characteristics of files. This allows you to not only block threats but to understand threat behavior to further mitigate or respond to threats.

Cylance score

The Cylance score represents the confidence level that the file poses a real danger to your environment. The higher the score, the greater the confidence level that the file can be used for malicious purposes. Based on the score, threats are considered either unsafe or abnormal.

Files that are identified as a potential threat will have their score displayed in red (unsafe or abnormal). Files that are identified as safe will have their score displayed in green. Under normal circumstances you will not see safe (green) files displayed in the console. Safe files that are shown in the console are typically displayed when the file has been added to your global quarantine list and quarantined on a device.

Files that would be considered unsafe/abnormal (red score) are treated as safe if you add the files to your global safe list and will not be displayed in the console.

Occasionally, a file may be classified as either unsafe or abnormal even if the score displayed doesn’t match the range for the score. This may be due to update findings or additional file analysis that may have been performed after the initial detection. For the most up-to-date threat analysis, enable auto upload in the policy.

The Cylance score is independent of threat classification. Most threat classifications are a manual process that is undertaken by a human threat researcher and assigned on a file-by-file basis. It is possible for a file to have a Cylance score but not have a classification until a later date.

Unsafe and abnormal files

BlackBerry groups CylancePROTECT Desktop threat alerts using the Cylance score for the threat. This helps simplify actions like automatically adding unsafe and abnormal threats to the global quarantine list using a device policy.

- **Unsafe:** A file with a score ranging from 60-100. An unsafe file is one that has attributes that greatly resemble malware.
- **Abnormal:** A file with a score ranging from 1-59. An abnormal file has a few malware attributes but less than an unsafe file and is less likely to be malware.

Occasionally, a file may be classified as unsafe or abnormal even though the score displayed does not match the range for the classification. This could result from updated findings or additional file analysis after the initial detection. For the most up-to-date analysis, enable auto upload in the device policy.

File classification

The following table lists the possible file status entries that could display for each CylancePROTECT Desktop threat.

File Status	Description
File Unavailable	Due to an upload constraint (for example, the file is too large), the file is not available for analysis. Contact BlackBerry Support for an alternate method to transfer the file.
Blank entry	The file has not yet been analyzed. When an analysis is complete, a new status will be assigned.
Trusted - Local	The file is considered to be safe. You can add the file to the global safe list so that it will be allowed to execute and will not generate alerts when it is identified on other devices.
PUP	The file is a Potentially Unwanted Program (PUP), indicating that it might be unsafe even if a user consented to downloading it. Some PUPs may be permitted to run on a limited set of systems in your organization (for example, a VNC application that is allowed to run on domain administrator devices). You can choose to waive or block PUPs on a per device basis, or add it to the global quarantine or safe list based on your organization's standards. The file can have any of the following sub-classes: • Adware • Corrupt • Game • Generic • Hacking Tool • Portable Application (does not require installation) • Scripting Tool • Toolbar

File Status	Description
Dual Use	The file can be used for malicious and non-malicious purposes. For example, while PsExec can be a useful tool for executing processes on another system, that same feature can be used to execute malicious files on another system. The file can have any of the following sub-classes: • Crack (alters another application to bypass licensing limitations) • Generic • KeyGen (generate, reveal, or recover product keys) • Monitoring Tool • Pass Crack • Remote Access • Tool (administrative programs that can facilitate an attack)
Malware	The file has been identified as malicious software that is designed to disrupt, damage, or gain unauthorized access to your network, and should be removed as soon as possible. The file can have any of the following sub-classes: • Backdoor • Bot • Downloader • Dropper • Exploit • FakeAlert • Generic • InfoStealer • Parasitic • Ransom • Remnant • Rootkit • Trojan • Virus • Worm
Possible Malware	The file has been identified as suspicious software and is considered to be abnormal or unsafe. You can add it to the global quarantine list or safe list based on your organization's standards.

Evaluate the risk level of a file

You can use the management console to evaluate the risk level of a file, as analyzed and determined by the CylancePROTECT cloud services. This feature gives you insight into how the CylancePROTECT Desktop agent would classify a file that it identifies on a device. Currently, Windows, macOS, and Linux executables are supported.

Before you begin: You must have the Administrator role to access this feature in the console.

1. In the management console, on the menu bar, click **Protection > Threat Analysis**.
2. Do one of the following:

Action	Steps
Look up a file by hash.	In the **Hashes** field, type or paste SHA256 hashes, separating each hash on a new line. You can add up to 32 hashes.
Upload a file.	The maximum size of a file that you can upload is 10 MB. **a.** On the **Upload File** tab, click **Browse Files**. **b.** Navigate to and select the file that you want to analyze. Click **Open**.

3. Click **Analyze**.
4. Review the file status to determine whether a threat was found or if the file is considered safe.

   If you receive a **File Required** status after you lookup a file by the SHA256 hash, upload the file on the **Upload File** tab.

After you finish: If necessary, add a file to the global quarantine list or to the global safe list. For instructions, see Add a file to the CylancePROTECT Desktop global quarantine or global safe list.

Using CylancePROTECT Desktop reports

On the menu bar, you can click Reports to view the following CylancePROTECT Desktop reports. The reports are interactive, allowing you to select pieces of data to view further details.

Report	Description
CylancePROTECT overview	This report provides an executive summary of CylancePROTECT Desktop usage, including a count of zones and devices, the percentage of devices covered by auto-quarantine and memory protection, and summaries of threat events, memory violations, agent versions, and an offline count for CylancePROTECT Desktop devices.
Threat event summary	This report shows the number of files identified as malware or potentially unwanted programs (PUPs) and includes a breakdown of specific sub-categories. The top ten lists for file owners and devices with threats display threat event counts for the malware, PUPs, and dual use threat families.
Device summary	This report displays summary data for CylancePROTECT Desktop devices.
Threat events	This report provides detailed data for threat events identified by the CylancePROTECT Desktop agent.
Devices	This report displays a count of CylancePROTECT Desktop devices by OS.

Reports display threats in an event-based manner. An event represents an individual instance of a threat. For example, if a particular file is in three different folder locations on a device, the threat event count will equal three. Reporting data is refreshed approximately every three minutes. You can export the CylancePROTECT overview, threat event summary, and device summary reports as a .png file, and the threat events and devices reports as a .csv file.

Retrieving threat data reports with a third-party application

You can also access and download detailed threat data reports using the URLs listed in the Threat Data Report section in Settings > Application. The URLs use a unique token that is generated by the management console and displayed in Settings > Application. You can delete and regenerate the token as necessary. Note that regenerating the token will make previous tokens invalid. If you want to use a third-party application to retrieve reports from these URLs, the application and the host OS must use:

- TLS 1.2
- The ciphers supported by the TLSv1.2_2021 policy

Managing threats detected by CylancePROTECT Mobile

You can use the management console to view a collective list of the mobile threats that the CylancePROTECT Mobile app has detected on users' devices. Alerts are stored for up to 120 days. If you disable the CylancePROTECT Mobile service for a user, any alerts associated with that user are removed from the management console.

View CylancePROTECT Mobile alerts

1. In the management console, on the menu bar, click **Protection > Protect Mobile Alerts**.

   For more information about the CylancePROTECT Mobile alerts that can display on this screen, see Mobile threats detected by the CylancePROTECT Mobile app.
2. Optionally, do any of the following:
   - To view available details for an alert (for example, the detection time or first installation time), click the alert.
   - To group alerts, click the **Group by** drop-down list and click an option.
   - To sort the alerts in ascending or descending order by a column, click the name of the column.
   - To filter the alerts, click ≡ on a column and type or select the filter criteria.
   - To ignore one or more alerts, select the alerts and click **Ignore**. Click **Ignore** again to confirm.
   - To export the results to a .csv file, click ➡. Click **Export**.

You can use the following information to add an app or certificates to the CylancePROTECT Mobile safe or restricted list:

- For iOS sideloaded app threats, the **Name** column displays the common name of the developer certificate.
- For Android malicious and sideloaded app threats, the **Description** column displays the SHA256 hash of the app.

Mobile threats detected by the CylancePROTECT Mobile app

The following table lists the possible alerts that can be reported in the management console in Protection > Protect Mobile Alerts:

Mobile security threat	UI alert type	UI alert name	UI description
App security: Malicious apps	Malicious app	App name	Package name, package version, SHA256 hash
App security: Sideloaded apps	Sideloaded app	Android: App name iOS: Signing identity	Android: Package name, package version, installer source, SHA256 hash
App security: Restricted apps	Restricted app	Android: App name iOS: Signing identity	Android: Package name, package version, installer source, SHA256 hash

Mobile security threat	UI alert type	UI alert name	UI description
Network protection: Wi-Fi security	Insecure Wi-Fi	Network SSID If disabled by the user: Feature disabled by user	Wi-Fi access algorithms
Network protection: Network connection	Compromised network	Network type	Network SSID
Device security: Unsupported device model	Unsupported device model	Model name	NA
Device security: Unsupported OS	Unsupported OS	OS name, OS version	NA
Device security: Unsupported security patch	Unsupported security patch	Patch version When attestation certificate verification fails: Untrusted	NA
Device security: Root/Jailbreak detection	Compromised device	Android: Rooted iOS: Jailbroken	OS name, OS version
Device security: Full disk encryption	Encryption disabled	Encryption disabled	OS name, OS version
Device security: Screen lock	Screen lock disabled	Screenlock disabled	OS name, OS version
Device security: Developer options	Developer mode	Developer mode is enabled	OS name, OS version
Device security: Android SafetyNet or Play Integrity attestation	SafetyNet or Play Integrity attestation failure	Android SafetyNet Android Play Integrity	Attestation type, attestation state
Device security: Android hardware certificate attestation	Hardware attestation failure	Android Hardware	Hardware key attestation: attestation type, attestation state, rule failure Other detections: attestation type, attestation state
Device security: Samsung Knox Enhanced Attestation	Knox Enhanced Attestation failure	Knox Enhanced Attestation	Knox, Device Failure

Mobile security threat	UI alert type	UI alert name	UI description
Device security: iOS integrity check	App integrity attestation failure	iOS App Integrity Check	Attestation type, attestation state
Message scanning (displays for Android only)	Unsafe message	Malicious SMS	List of malicious URLs

Managing safe and unsafe lists for CylancePROTECT Desktop and CylancePROTECT Mobile

This section provides information for adding files and certificates to quarantine or safe lists for CylancePROTECT Desktop, and adding apps, developer certificates, IP addresses, and domains to safe or restricted lists for CylancePROTECT Mobile.

Add a file to the CylancePROTECT Desktop global quarantine or global safe list

You can add a file to the global quarantine list to block it from all CylancePROTECT Desktop devices. Add a file to the global safe list to allow it on all CylancePROTECT Desktop devices. The unassigned list is for files listed in the management console that have not been globally quarantined or safe listed.

To add files to a local quarantine or local safe list for a device, see Add a file to the CylancePROTECT Desktop local quarantine or local safe list.

Do any of the following:

Task	Steps
Add a file to the global quarantine or safe list from the threats page.	**a.** In the management console, on the menu bar, click **Protection > Threats**. **b.** Select the file. **c.** Do one of the following: • To add the file to the global quarantine list, click **Global Quarantine**. • To add the file to the global safe list, click **Safe**. **d.** Specify the required information. **e.** Click **Yes**.
Add a file to a global quarantine or safe list manually.	**a.** In the management console, on the menu bar, click **Settings > Global List**. **b.** Click the **Global Quarantine** or **Safe** tab. **c.** Click **Add File**. **d.** Specify the file information. **e.** Click **Submit**.
Add a file to the global quarantine or safe list from the unassigned list.	**a.** In the management console, on the menu bar, click **Settings > Global List**. **b.** On the **Unassigned** tab, select the file. **c.** Do one of the following: • To add the file to the global quarantine list, click **Global Quarantine**. • To add the file to the global safe list, click **Safe**. **d.** Specify a reason for adding the file to the global list. **e.** Click **Yes**.

Task	Steps
Move a file from one global list to another.	**a.** In the management console, on the menu bar, click **Settings > Global List**. **b.** Click the **Global Quarantine** or **Safe** tab. **c.** Select the file that you want to move. **d.** Do one of the following: • To move the file to the global quarantine list, click **Global Quarantine**. • To move the file to the global safe list, click **Safe**. • To move the file to the unassigned list, click **Remove from list**. **e.** Specify the required information. **f.** Click **Yes**.

Add a file to the CylancePROTECT Desktop local quarantine or local safe list

Add a file to the local quarantine list to block it from that device. Add a file to the local waive list (local safe) for that device. These actions affect the device only, it does not affect any other devices in the organization.

To add files to the CylancePROTECT Desktop global quarantine or global safe list, see Add a file to the CylancePROTECT Desktop global quarantine or global safe list.

1. In the management console, on the menu bar, click **Assets > Devices**.
2. Click a device.
3. Under **Threats**, select the file.
4. Click **Quarantine** to add the file to the local quarantine list. Click **Waive** to add the file to the local waive list (local safe).
5. Enter any required information.
6. Click **Yes**.

Add a certificate to the CylancePROTECT Desktop global safe list

For custom software that is properly signed, add the certificate to the certificates list to allow the software to run without interruption. This allows administrators to create a safe list by signed certificate which is represented by the SHA1 thumbprint of the certificate. When adding certificate information to the management console, the certificate itself is not uploaded or saved to the management console; the certificate information is extracted and saved to the management console (timestamp, subject, issuer, and thumbprint). The certificate timestamp represents when the certificate was created. The management console does not check if the certificate is current or expired. If the certificate changes (for example, renewed or new), it should be added to the safe list in the management console. The safe list by certificate feature works with PowerShell, ActiveScript, and Office macros.

This feature currently works with Windows and macOS only.

Before you begin: Identify the certificate thumbprint for the signed Portable Executable (PE).

1. In the management console, on the menu bar, click **Settings > Certificates**.
2. Click **Add Certificate**.
3. Click either **Browse for certificates to add** or drag-and-drop the certificate to the message box. If browsing for the certificates, the Open window displays to allow selection of the certificates.

4. Optionally, you can select the file type the certificate **Applies to**, Executable, or Script. This allows you to add an executable or script by a certificate instead of a folder location.
5. Optionally, add notes about the certificate.
6. Click **Submit**. The Issuer, Subject, Thumbprint, and Notes (if entered) are added to the repository.

Add an app, certificate, IP address, domain, or installer source to the CylancePROTECT Mobile safe or restricted list

You can use the CylancePROTECT Mobile safe and restricted lists to manage the following:

- Exempt a specific app or developer signing certificate from malware and sideload detection.
- Classify a specific app or developer signing certificate as a threat for malware and sideload detection.
- Exempt an IP address or domain from message scanning.
- Classify a specific IP address or domain as a threat for message scanning.
- Exempt a specific installer source from sideload detection.
- Classify a specific installer source as a threat for sideload detection.

Before you begin:

- In **Protection > Protect Mobile Alerts**, you can click alerts to view details such as the app hash, certificate details, package details, and so on. You might need this information when you follow the steps below to add items to the safe or restricted list.
- If you want to add an Android developer certificate to the safe or restricted list, you must get the thumbprint of the certificate from the app binary. For instructions, see KB 70577.

1. In the management console, on the menu bar, click **Settings > Global List (Mobile)**.
2. Do any of the following:

Task	Steps
Add a developer certificate to the malware and sideload detection safe list.	**a.** On the **Safe** tab, click **Developers**. **b.** Click **Add Certificate**. **c.** Do one of the following: • To add the signing certificate from an app file, click **Select an app to get certificate information**. Browse to and select the .apk or .ipa file and click **Submit**. • To manually enter the certificate information, click **Manually enter certificate information**. Specify the certificate details and click **Add**. • To import a list of certificates from a .csv file, click **Import certificate list from .csv file**. Browse to and select the file and click **Upload**.

Task	Steps
Add a developer certificate to the malware and sideload detection restricted list. (Android only)	**a.** On the **Restricted** tab, click **Developers**. **b.** Click **Add Certificate**. **c.** Do one of the following: • To add the signing certificate from an app file, click **Select an app to get certificate information**. Browse to and select the .apk file and click **Submit**. • To manually enter the certificate information, click **Manually enter certificate information**. Specify the certificate details and click **Add**. • To import a list of certificates from a .csv file, click **Import certificate list from .csv file**. Browse to and select the file and click **Upload**.
Add an app to the malware and sideload detection safe list.	**a.** On the **Safe** tab, click **Apps**. **b.** Click **Add App**. **c.** Do one of the following: • To add an app file, click **Select an app file**. Browse to and select the .apk or .ipa file and click **Submit**. • To manually enter the app hash, click **Manually enter the app's hash info**. Specify the app details and click **Add**. • To import a list of apps from a .csv file, click **Import an app list from .csv file**. Browse to and select the file and click **Upload**. **Note:** If an app contains multiple .apk files, you must manually enter the hash of each file. Optionally, you can add the app's signing certificate instead.
Add an app to the malware detection restricted list. (Android only)	**a.** On the **Restricted** tab, click **Apps**. **b.** Click **Add App**. **c.** Do one of the following: • To add an app file, click **Select an app file**. Browse to and select the .apk file and click **Submit**. • To manually enter the app hash, click **Manually enter the app's hash info**. Specify the app details and click **Add**. • To import a list of apps from a .csv file, click **Import an app list from .csv file**. Browse to and select the file and click **Upload**. **Note:** If an app contains multiple .apk files, you must manually enter the hash of each file. Optionally, you can add the app's signing certificate instead.
Add an IP address to the message scanning safe list. (Android only)	**a.** On the **Safe** tab, click **IP Addresses**. **b.** Click **Add IP Address**. **c.** Do one of the following: • To manually enter the IP address, click **Manually enter IP address information**. Specify the IP details and click **Add**. • To import a list of IP addresses from a .csv file, click **Import IP address list from .csv file**. Browse to and select the file and click **Upload**.

Task	Steps
Add an IP address to the message scanning restricted list. (Android only)	**a.** On the **Restricted** tab, click **IP Addresses**. **b.** Click **Add IP Address**. **c.** Do one of the following: • To manually enter the IP address, click **Manually enter IP address information**. Specify the IP details and click **Add**. • To import a list of IP addresses from a .csv file, click **Import IP address list from .csv file**. Browse to and select the file and click **Upload**.
Add a domain to the message scanning safe list. (Android only)	**a.** On the **Safe** tab, click **Domains**. **b.** Click **Add Domain**. **c.** Do one of the following: • To manually enter the domain information, click **Manually enter domain information**. Specify the domain details and click **Add**. • To import a list of domains from a .csv file, click **Import domain list from .csv file**. Browse to and select the file and click **Upload**.
Add a domain to the message scanning restricted list. (Android only)	**a.** On the **Restricted** tab, click **Domains**. **b.** Click **Add Domain**. **c.** Do one of the following: • To manually enter the domain information, click **Manually enter domain information**. Specify the domain details and click **Add**. • To import a list of domains from a .csv file, click **Import domain list from .csv file**. Browse to and select the file and click **Upload**.
Add an installer source to the sideload detection safe list.	**a.** On the **Safe** tab, click **Installer Sources**. **b.** Click **Add Installer Source**. **c.** Do one of the following: • To manually enter the installation source information, click **Manually enter installation source information**. Specify the details and click **Add**. • To import a list of installer sources from a .csv file, click **Import installation source list from .csv file**. Browse to and select the file and click **Upload**.
Add an installer source to the sideload detection restricted list.	**a.** On the **Restricted** tab, click **Installer Sources**. **b.** Click **Add Installer Source**. **c.** Do one of the following: • To manually enter the installation source information, click **Manually enter installation source information**. Specify the details and click **Add**. • To import a list of installer sources from a .csv file, click **Import installation source list from .csv file**. Browse to and select the file and click **Upload**.

After you finish:

- To remove an item from any of the safe or restricted lists, select it and click **Delete**. When you are prompted, click **Delete** again.
- To export any of the safe or restricted lists, click ➔. Click **Export** to confirm.

Analyzing data collected by CylanceOPTICS

This section provides information about how you can view, analyze, and use the data collected by CylanceOPTICS.

CylanceOPTICS sensors

The following sensors are enabled by default in the CylanceOPTICS agent when you turn on CylanceOPTICS in a device policy. You cannot disable these sensors. For more information about the optional sensors that you can enable, see CylanceOPTICS optional sensors.

For more information about the events, artifacts, and event types associated with both the default and optional sensors, see Data structures that CylanceOPTICS uses to identify threats.

Sensor	Platform	Description	Event types
Device	macOS Linux	Collects relevant device information	Mount
File	Windows macOS Linux	Collects information about file operations	• Create • Delete • Overwrite • Rename • Write
Memory	macOS Linux	Collects information about memory operations	• Mmap • MProtect
Network	Windows macOS Linux	Collects information about network connections	Connect
Process	Windows macOS Linux	Collects information about process operations	Supported event types differ by platform. See the Process section of Data structures that CylanceOPTICS uses to identify threats. • Abnormal Exit • Exit • Forced Exit • PTrace • Start • Suspend • Unknown Linux Process Event

Sensor	Platform	Description	Event types
Registry	Windows	Collects information about registry operations	• KeyCreated • KeyDeleting • ValueChanging • ValueDeleting

CylanceOPTICS optional sensors

You can enable any of the following CylanceOPTICS sensors to collect additional data beyond standard process, file, network, and registry events. Enabling optional sensors can impact performance and resource usage on devices, as well as the amount of data stored in the CylanceOPTICS database. BlackBerry recommends enabling optional sensors on a small number of devices initially to assess the impact.

The optional sensors are supported for 64-bit operating systems only, unless otherwise noted.

Sensor	Description	Best practices	Notes
Advanced Scripting Visibility	The CylanceOPTICS agent records commands, arguments, scripts, and content from JScript, PowerShell (console and integrated scripting environment), VBScript, and VBA macro script execution. Signal to noise ratio: High Potential data retention and performance impact: Low to moderate	Recommended for: • Desktops • Laptops • Servers Not recommended for Microsoft Exchange and email servers.	• Tools provided by Microsoft or other third-party solutions may rely heavily on PowerShell to conduct operations. • To allow for increased data retention, BlackBerry recommends that you configure detection exceptions for trusted tools that make heavy use of PowerShell.
Advanced WMI Visibility	The CylanceOPTICS agent records additional WMI attributes and parameters. Signal to noise ratio: High Potential data retention and performance impact: Low	Recommended for: • Desktops • Laptops • Servers	• Some Windows background and maintenance processes use WMI to schedule tasks or execute commands, which can result in bursts of high WMI activity. • BlackBerry recommends analyzing your environment's WMI usage before you enable this sensor.

Sensor	Description	Best practices	Notes
API Sensor	The CylanceOPTICS agent monitors an identified set of Windows API calls. Signal to noise ratio: Moderate Potential data retention and performance impact: Enabling this sensor may impact a device's CPU performance	Recommended for: • Desktops • Laptops • Servers	• Supported on x86 or x64 Windows operating systems. • Requires the CylancePROTECT Desktop agent version 3.0.1003 or later. • Requires the CylanceOPTICS agent version 3.2 or later.
COM Object Visibility	The CylanceOPTICS agent monitors COM interface and API calls to detect malicious behaviors such as scheduled task creation. Signal to noise ratio: High Potential data retention and performance impact: Enabling this sensor may impact CPU performance.	Recommended for: • Desktops • Laptops Not recommended for servers.	• Windows only. • Requires CylancePROTECT Desktop agent version 3.2 or later. • Requires the CylanceOPTICS agent version 3.3 or later.
Cryptojacking Detection	The CylanceOPTICS agent processes Intel CPU activity using hardware registers for potential cryptomining and cryptohacking activity. Signal to noise ratio: Moderate Potential data retention and performance impact: Low	Supported for: • Windows 10 x64 • Intel Gen 6 to 10	• Not supported for virtual machines. • Not supported for Intel Gen 11 or later processors. BlackBerry does not recommend enabling this sensor for Gen 11 or later.
DNS Visibility	The CylanceOPTICS agent records DNS requests, responses, and associated data fields such as Domain Name, Resolved Addresses, and Record Type. Signal to noise ratio: Moderate Potential data retention and performance impact: Moderate	Recommended for: • Desktops • Laptops Not recommended for DNS servers.	• Note that this sensor can gather a significant amount of data, but can also provide visibility into data that other tools have difficulty recording. • To allow for increased data retention, BlackBerry recommends that you configure detection exceptions for trusted tools that make heavy use of cloud-based services.

Sensor	Description	Best practices	Notes
Enhanced File Read Visibility	The CylanceOPTICS agent monitors file reads within an identified set of directories. Signal to noise ratio: Moderate Potential data retention and performance impact: Low	Recommended for: • Desktops • Laptops • Servers	• Some third-party security tools may use the Windows APIs that this sensor collects data from. In some cases, CylanceOPTICS might record irrelevant or trusted data. • To allow for increased data retention and a higher signal to noise ratio, BlackBerry recommends that you configure detection exceptions for trusted security tools.
Enhanced Portable Executable Parsing	The CylanceOPTICS agent records data fields associated with portable executable files, such as file version, import functions, and packer types. Signal to noise ratio: Moderate Potential data retention and performance impact: Low	Recommended for: • Desktops • Laptops • Servers	• The data gathered by this sensor is passed into the Context Analysis Engine to aid with advanced executable file analysis and is not stored in the CylanceOPTICS database. • Enabling this sensor will have little to no impact on CylanceOPTICS data retention. • If you add and enable a detection rule that analyzes string resources, the CylanceOPTICS agent might consume significant CPU and memory resources.
Enhanced Process and Hooking Visibility	The CylanceOPTICS agent records process information from the Win32 API and Kernel Audit messages to detect forms of process hooking and injection. Signal to noise ratio: Moderate Potential data retention and performance impact: Low	Recommended for: • Desktops • Laptops • Servers	• Some third-party security tools may use the Windows APIs that this sensor collects data from. In some cases, CylanceOPTICS might record irrelevant or trusted data. • To allow for increased data retention and a higher signal to noise ratio, BlackBerry recommends that you configure detection exceptions for trusted security tools.

Sensor	Description	Best practices	Notes
HTTP Visibility	The CylanceOPTICS agent tracks Windows HTTP transactions, including Event Tracing for Windows, WinINet APIs, and WinHTTP APIs. Signal to noise ratio: High Potential data retention and performance impact: Enabling this sensor may impact CPU performance.	Recommended for: • Desktops • Laptops Not recommended for servers.	• Windows only. • Requires CylancePROTECT Desktop agent version 3.2 or later. • Requires the CylanceOPTICS agent version 3.3 or later.
Module Load Visibility	The CylanceOPTICS agent monitors module loads. Signal to noise ratio: High Potential data retention and performance impact: Enabling this sensor may impact CPU performance.	Recommended for: • Desktops • Laptops • Servers	• Windows only. • Requires CylancePROTECT Desktop agent version 3.2 or later. • Requires the CylanceOPTICS agent version 3.3 or later.
Private Network Address Visibility	The CylanceOPTICS agent records network connections within the RFC 1918 and RFC 4193 address spaces. Signal to noise ratio: Low Potential data retention and performance impact: Low	Recommended for desktops. Not recommended for: • DNS servers • Low or under resourced systems • Systems that use RDP or other remote access software	• This sensor gathers a significant amount of data and can impact the length of time that data is stored in the CylanceOPTICS database. • BlackBerry recommends that you enable this sensor only in environments where full visibility into private network address communication is a requirement.
Windows Advanced Audit Visibility	The CylanceOPTICS agent monitors additional Windows event types and categories. Signal to noise ratio: Moderate Potential data retention and performance impact: Low	—	This sensor enables monitoring of the following event IDs: • 4769 kerberos ticket request • 4662 operation on active directory object • 4624 successful logon • 4702 scheduled task creation

Sensor	Description	Best practices	Notes
Windows Event Log Visibility	The CylanceOPTICS agent records Windows security events and their associated attributes. Signal to noise ratio: Moderate Potential data retention and performance impact: Moderate	Recommended for: • Desktops • Laptops • Servers Not recommended for: • Domain controllers • Microsoft Exchange and email servers	• The Windows event logs that this sensor collects data from will be generated frequently during normal system usage. • To reduce duplicate data and to allow for increased data retention, determine if your organization already has tools in place that collect data from Windows event logs.

Data structures that CylanceOPTICS uses to identify threats

Events, artifacts, and facets are the three primary data structures that CylanceOPTICS uses to analyze, record, and investigate activities that occur on devices. CylanceOPTICS features rely on these data structures, including InstaQuery, focus data, and the Context Analysis Engine (CAE).

This section provides more information about how CylanceOPTICS interprets and interacts with activities on devices, to help you better understand and make use of detections, queries, and focus data.

Data sources by OS

The CylanceOPTICS agent uses the following data sources:

OS	Data sources
Windows	• CyOpticsDrv kernel driver • Event tracking • Security audit log
macOS	CyOpticsDrvOSX kernel driver
Linux	ZeroMQ

For information about the types of network traffic that CylanceOPTICS excludes by default, see KB65604.

Events

Events are the components that result in an observable change or action on a device. Events consist of two primary artifacts: the instigating artifact that initiates an action, and the target artifact that is acted on.

The following tables provide details about the types of events that CylanceOPTICS can detect and interact with.

Event: Any

- Device policy option to enable: CylanceOPTICS check box

- Artifact type: Process, User
- Platform: Windows, macOS, Linux

Event type	Description
Any	All events record the process that generated them and the user that is associated with the action.

Event: Application

- Device policy option to enable: Advanced WMI Visibility
- Artifact type: WMI trace
- Platform: Windows

Event type	Description
Create Filter-Consumer Binding	A process used WMI persistence.
Create Temporary Consumer	A process subscribed to WMI events.
Execute Operation	A process performed a WMI operation.

- Device policy option to enable: Enhanced Process and Hooking Visibility
- Artifact type: File
- Platform: Windows

Event type	Description
CBT	The SetWindowsHookEx API installed a hook to receive notifications that are useful to a CBT application.
DebugProc	The SetWindowsHookEx API installed a hook to debug other hook procedures.
Get Async Key State	A process called the Win32 GetAsyncKeyState API.
JournalPlayback	The SetWindowsHookEx API installed a hook to monitor messages previously recorded by a WH_JOURNALRECORD hook procedure.
JournalRecord	The SetWindowsHookEx API installed a hook to monitor input messages posted to the system message queue.
Keyboard	The SetWindowsHookEx API installed a hook to monitor keystroke messages.
LowLevel Keyboard	The SetWindowsHookEx API installed a hook to monitor low-level keyboard input events.
LowLevel Mouse	The SetWindowsHookEx API installed a hook to monitor low-level mouse input events.

Event type	Description
Message	The SetWindowsHookEx API installed a hook to monitor messages posted to a message queue.
Mouse	The SetWindowsHookEx API installed a hook to monitor mouse messages.
Register Raw Input Devices	A process called the Win32 RegisterRawInputDevices API.
Set Windows Event Hook	A process called the Win32 SetWinEventHook API.
Set Windows Hook	The SetWindowsHookEx API installed an unlisted hook type value.
ShellProc	The SetWindowsHookEx API installed a hook to receive notifications that are useful to shell applications.
SysMsg	The SetWindowsHookEx API installed a hook to monitor messages that are generated as a result of an input event in a dialog box, message box, or scroll bar.
WindowProc	The SetWindowsHookEx API installed a hook to monitor Windows procedure messages.

- Device policy option to enable: API Sensor
- Artifact type: API Call
- Platform: Windows

Event type	Description
Function	A noteworthy function call has been made.

- Device policy option to enable: Module Load Visibility
- Artifact type: File
- Platform: Windows

Event type	Description
Load	An application loaded a module.

- Device policy option to enable: COM Object Visibility
- Platform: Windows

Event type	Description
Created	A COM object was created.

Event: Device

- Device policy option to enable: CylanceOPTICS check box
- Artifact type: File
- Platform: macOS, Linux

Event type	Description
Mount	The device is connected to a machine or folders are mounted to specific network locations.

Event: File

- Device policy option to enable: CylanceOPTICS check box
- Artifact type: File
- Platform: Windows, macOS, Linux

Event type	Description
Create	A file was created.
Delete	A file was deleted.
Overwrite	A file was overwritten.
Rename	A file was renamed.
Write	A file was modified.

- Device policy option to enable: Enhanced File Read Visibility
- Artifact type: File
- Platform: Windows

Event type	Description
Open	A file was opened.

Event: Memory

- Device policy option to enable: CylanceOPTICS check box
- Artifact type: Process
- Platform: macOS, Linux

Event type	Description
Mmap	A region of memory was mapped for a specific purpose, typically allocated for a process.
MProtect	The metadata was changed for a region of memory, typically to change its status (for example, to make it executable).

Event: Network

- Device policy option to enable: CylanceOPTICS check box
- Artifact type: Network
- Platform: Windows, macOS

Event type	Description
Connect	A network connection was opened. By default, local traffic is not collected.

- Device policy option to enable: Private Network Address Visibility
- Artifact type: Network
- Platform: Windows

Event type	Description
Connect	Connect events include local traffic.

- Device policy option to enable: DNS Visibility
- Artifact type: DNS request
- Platform: Windows

Event type	Description
Request	A process made a network DNS request that was not cached.
Response	A process received a DNS response.

- Device policy option to enable: HTTP Visibility
- Artifact type: HTTP
- Platform: Windows

Event type	Description
Get	Windows used WinINet or WinHTTP to make an HTTP request.
Post	Windows used WinINet or WinHTTP to send data.

Event: Process

- Device policy option to enable: CylanceOPTICS check box
- Artifact type: Process

Event type	Platform	Description
Abnormal Exit	macOS Linux	Monitored by the preselect sensor, a process exited without completing (for example, an exception caused a process to exit).
Exit	Windows macOS Linux	A process exited.
Forced Exit	macOS Linux	Monitored by the preselect sensor, a process was forced to exit by another process.

Event type	Platform	Description
PTrace	macOS Linux	This is a Unix system tool that allows one process to monitor and control another process.
Start	Windows macOS Linux	A process started.
Suspend	Linux	Monitored by the preselect sensor, a process was suspended.
Unknown Linux Process Event	macOS Linux	Monitored by the preselect sensor, an unknown event occurred with the process as a target. This can be a sign of malicious software masking its activity.

- Device policy option to enable: Enhanced Process and Hooking Visibility
- Artifact type: Process
- Platform: Windows

Event type	Description
SetThreadContext	A process called the SetThreadContext API.
Terminate	An instigating process terminated another target process.

Event: Registry

- Device policy option to enable: CylanceOPTICS check box
- Artifact type: Registry, File (if the registry key references a specific file)
- Platform: Windows

Event type	Description
KeyCreated	A registry key was created.
KeyDeleting	A registry key was deleted.
ValueChanging	The value of a registry key was changed.
ValueDeleting	A registry key value was deleted.

Event: Scripting

- Device policy option to enable: Advanced Scripting Visibility
- Artifact type: Powershell Trace
- Platform: Windows

Event type	Description
Execute Command	Windows PowerShell executed a command. The parameters are unknown.

Event type	Description
Execute Script	Windows PowerShell executed a script.
Execute ScriptBlock	Windows PowerShell executed a script block.
Invoke Command	Windows PowerShell invoked a command with bound parameters.
Prevent Script	An AMSI ScanBuffer result indicated that a script was detected or blocked by an administrator.

Event: User

- Device policy option to enable: Advanced Scripting Visibility
- Artifact type: Windows Event
- Platform: Windows

Event type	Description
Batch Logoff	The following Windows event ID occurred: 4634 (type 4).
Batch Logon	The following Windows event ID occurred: 4624 (type 4).
CachedInteractive Logoff	The following Windows event ID occurred: 4634 (type 11).
CachedInteractive Logon	The following Windows event ID occurred: 4624 (type 11).
Interactive Logoff	The following Windows event ID occurred: 4634 (type 2).
Interactive Logon	The following Windows event ID occurred: 4624 (type 2).
Network Logoff	The following Windows event ID occurred: 4634 (type 3).
Network Logon	The following Windows event ID occurred: 4624 (type 3).
NetworkClearText Logoff	The following Windows event ID occurred: 4634 (type 8).
NetworkClearText Logon	The following Windows event ID occurred: 4624 (type 8).
NewCredentials Logoff	The following Windows event ID occurred: 4634 (type 9).
NewCredentials Logon	The following Windows event ID occurred: 4624 (type 9).
RemoteInteractive Logoff	The following Windows event ID occurred: 4634 (type 10).

Event type	Description
RemoteInteractive Logon	The following Windows event ID occurred: 4624 (type 10).
Service Logoff	The following Windows event ID occurred: 4634 (type 5).
Service Logon	The following Windows event ID occurred: 4624 (type 5).
Unlock Logoff	The following Windows event ID occurred: 4634 (type 7).
Unlock Logon	The following Windows event ID occurred: 4624 (type 7).
User Logoff	The following Windows event ID occurred: 4634 (unlisted type value).
User Logon	The following Windows event ID occurred: 4624 (unlisted type value).

Artifacts and facets

Artifacts are complex pieces of information that CylanceOPTICS can use. The Context Analysis Engine (CAE) can identify artifacts on devices and use them to trigger automatic incident response and remediation actions. InstaQueries use artifacts as the foundation of a query.

Facets are the attributes of an artifact that can be used to identify the traits of an artifact that is associated with an event. Facets are correlated and combined during analysis to identify potentially malicious activity. For example, a file named "explorer.exe" may not be inherently suspicious, but if the file is not signed by Microsoft, and resides in a temporary directory, it may be identified as suspicious in some environments.

CylanceOPTICS uses the following artifacts and facets:

Artifact	Facets
API Call	• Function • DLL • Parameters
DNS	• Connection • IsRecursionDesired • IsUnsolicitedResponse • Opcode • RequestId • Resolution • ResponseOriginatedFromThisDevice • Questions
Event	• Occurrence time • Registration time

Artifact	Facets
File	• Executable file record (binaries only) • File creation time (reported by OS) • File path • File signature (binaries only) • File size • Last modified time (reported by OS) • md5 hash (binaries only) • Recent write location • sha256 hash (binaries only) • Suspected file type • User
Network	• Local address • Local port • Protocol • 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 (for example, SID) • Username User artifacts can contain any of the following values; however, the data is not available on most devices: • AccountType • BadPasswordCount • Comment • CountryCode • FullName • HasPasswordExpired • HomeDirectory • IsAccountDisabled • IsLocalAccount • IsLockedOut • IsPasswordRequired • LanguageCodePage • LogonServer • PasswordAge • PasswordDoesNotExpire • ProfilePath • ScriptPath • UserPrivilege • Workstations
Windows event	• Class • Event ID • ObjectServer • PrivilegeList • Process ID • Process Name • Provider Name • Service • SubjectDomainName • SubjectLogonId • SubjectUserName • SubjectUserSid
WMI trace	• ConsumerText • ConsumerTextAnalysis • EventId • Namespace • Operation • OperationAnalysis • OriginatingMachineName

Registry keys and values

CylanceOPTICS monitors common persistence, process startup, and privilege escalation keys and values as well as the values shown in KB 66266.

To learn more about how CylanceOPTICS monitors persistence points in the registry, see KB 66357.

View devices that are enabled for CylanceOPTICS

You can view details and status information for all devices that are enabled for CylanceOPTICS, including the CylanceOPTICS agent version installed on the device, the device IP address, and assigned zones. You can use the device view to take action to manage potential threats.

If a device is offline for 90 days or more, it does not do not display in the console.

1. In the management console, on the menu bar, click **CylanceOPTICS > Devices**.
2. Click ☰ to filter the results to find a specific device or group of devices.
3. Do any of the following:

Task	Steps
View summary details for a device.	Click the device name.
View full details for a device and change device properties and assignments.	**a.** Under the **Details** column, click **View**. **b.** Under **Edit Device Properties**, you can change the device name, assigned device policy, assigned zones, CylanceOPTICS agent log level, and protection level. Click **Save**. **c.** In the **Threats & Activities** section, you can view details for the threats that the CylanceOPTICS agent has detected.
Lock a device.	See Lock a device.
Deploy a package to collect data from the device.	**a.** Click the device name. **b.** In the **Select Action** drop-down list, click **Package Deploy**. **c.** Follow the steps in Deploy a package to collect data from devices.
Start a remote response session to send commands to the device.	**a.** Click the device name. **b.** In the **Select Action** drop-down list, click **Remote Response**. **c.** Enter commands into the remote response session window. For more information, see Sending actions to a device.
Export a .csv file of all devices.	Click ⇥.

Using InstaQuery and advanced query to analyze artifact data

InstaQuery and advanced query are CylanceOPTICS features that allow you to analyze artifact data to discover indicators of compromise and to determine their prevalence on your organization's devices. The results of a query will not tell you about how or when an artifact was used, but they will indicate whether an artifact has ever been observed in a forensically significant way that can signal a threat to your organization's devices and data.

InstaQuery allows you to interrogate a set of devices about a specific type of forensic artifact, and allows you to determine whether an artifact exists on devices and how common that artifact is. Advanced query is an evolution of InstaQuery that provides more granular search capabilities using EQL syntax to enhance your ability to identify threats.

After you install and enable the CylanceOPTICS agent on a device, the agent collects artifacts and stores them in the CylanceOPTICS database. With CylanceOPTICS agent 2.x and earlier, the database is stored locally on the device. With CylanceOPTICS agent 3.0 and later, the agent automatically uploads and stores data in the CylanceOPTICS cloud database. When you create a query, forensically significant data is retrieved from the CylanceOPTICS database. You can view and explore the results in the management console.

For devices with CylanceOPTICS agent 2.x and earlier, a query can complete successfully only when a device is online. For devices with agent 3.0 and later, the device does not need to be online because the query will use the latest data available in the CylanceOPTICS cloud database.

A single query will display and retain a maximum of 10,000 results. The results of a query are retained for 60 days.

Note the following details about specific artifacts that you can query:

Artifact	Details
Files	You can query specific files that were created, modified, or deleted after the CylanceOPTICS agent was installed on the device. CylanceOPTICS focuses on files that can be used to execute content (for example, executable files, Microsoft Office documents, PDFs, and so on).
Network connections	You can perform queries against both IPv4 and IPv6 destination IP addresses. CylanceOPTICS discards private, non-routable, multicast, link-local, and loopback network traffic.
Processes	All processes are indexed in the CylanceOPTICS database, with the following restrictions: • Command lines are limited to 1 KiB 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 monitored
Registry keys	CylanceOPTICS monitors only persistence points and file deletion points. They are areas typically exploited by malware. For a detailed list of registry keys and values monitored by CylanceOPTICS, see KB66266. To learn more about how CylanceOPTICS monitors persistence points in the registry, see KB66357.

Create an InstaQuery

1. In the management console, on the menu bar, click **CylanceOPTICS > InstaQuery**.
2. Do one of the following:

Task	Steps
Create a new InstaQuery.	If you want to clone a previous query, expand the **Previous Queries** section, find the query, and click **Clone Query**. **a.** In the **Search Term** field, type a value that you want to search for (for example, a file name, hash, process, registry value, and so on). If you want to search for an exact match, select the **Exact Matching** check box. **b.** In the **Artifact** drop-down list, click an artifact type. **c.** In the **Facet** drop-down list, click the appropriate facet. **d.** In the **Zone** drop-down list, select one or more zones. **e.** Type a name and description for the query. **f.** Click **Submit Query**. **g.** The current status of the query is displayed in the **Previous Queries** section. When the query is complete, click **View Results**.
View a previous InstaQuery.	**a.** Expand the **Previous Queries** section. **b.** For the query that you want to view, click **View Results**.

3. In the **InstaQuery Results** section, you can expand the **Actions** menu to access the available actions for each result. Depending on the type of result, this can include:

    - Request and view focus data.
    - Globally quarantine a file. The file is displayed in **Settings > Global List > Global Quarantine**, in **Protection > Threats**, and in the **Threats** section of the device details.
    - Request and download a file. If path information is available for files associated with other artifact types, you can also download those files. The file is compressed and password-protected to ensure that it is not accidentally executed. The password is “infected”.

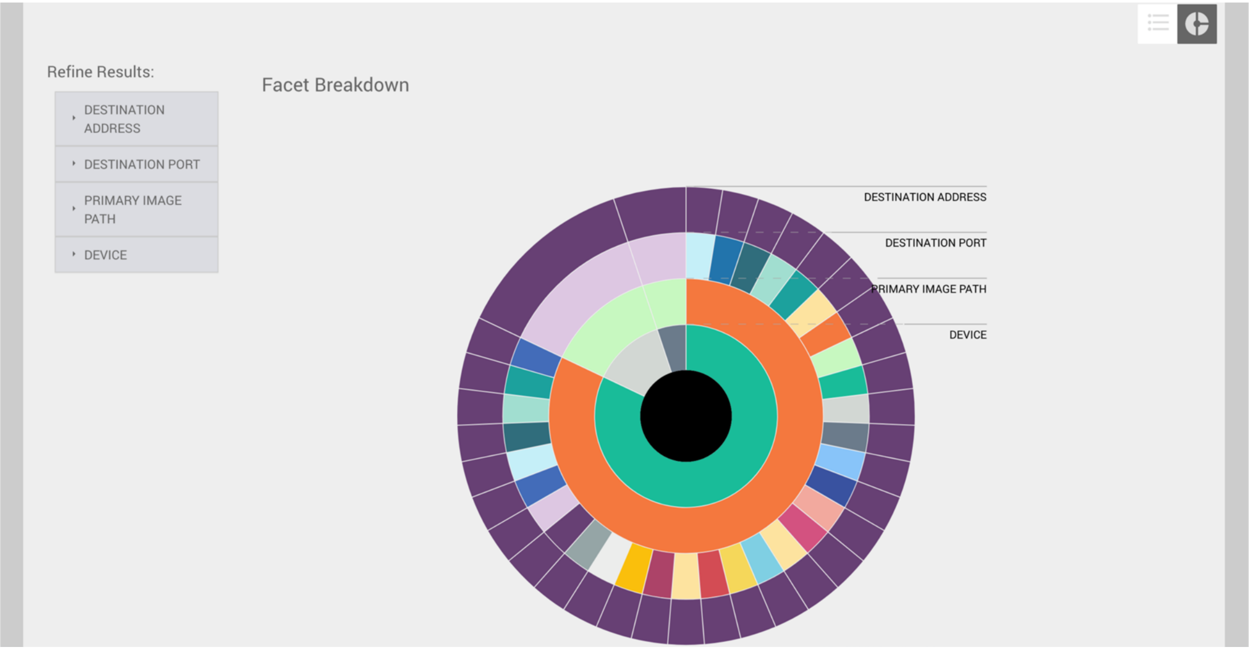
      The size limit for file retrieval is 50 MB. Artifacts and files are retained by CylanceOPTICS for 30 days (this period can be increased based on your organization's licensing).
4. To view the InstaQuery facet breakdown, in the **InstaQuery Results** section, click the facet breakdown icon.

Using the InstaQuery facet breakdown

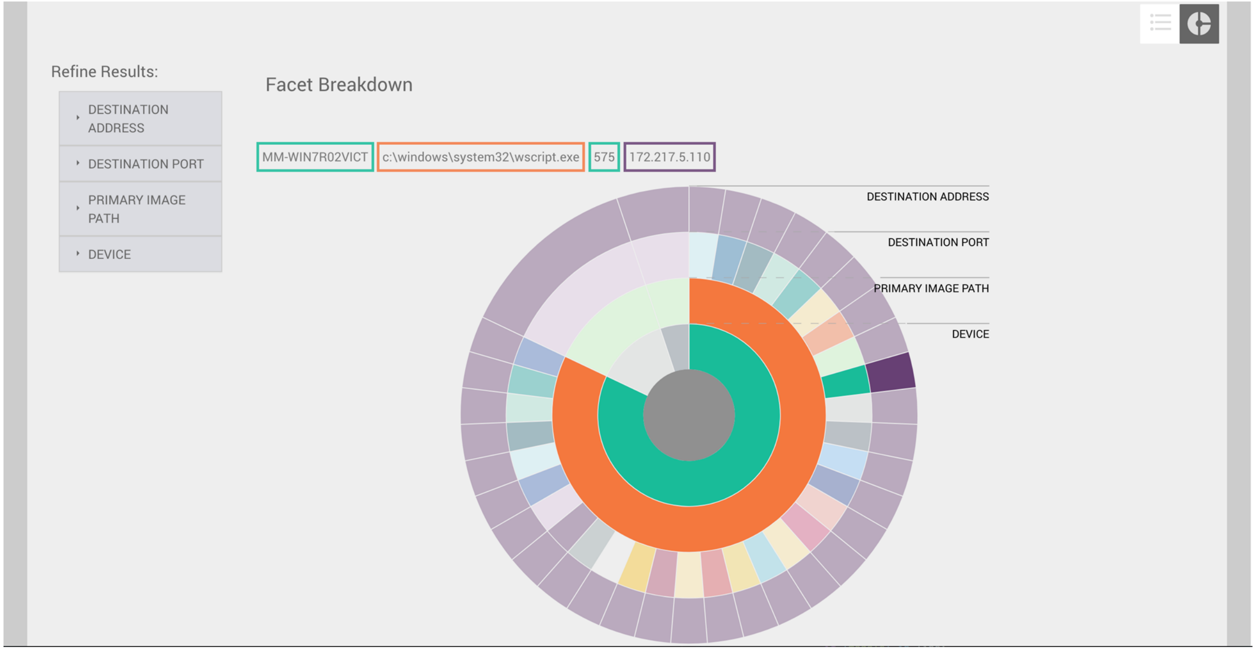
The InstaQuery facet breakdown provides an interactive visual display of the different facets involved in a query so that you can identify and follow their relational paths.

The sunburst model of the facet breakdown is useful for identifying suspicious activity in a given dataset. For example, if you try to find suspicious network connections across an environment or multiple zones, data patterns and anomalies can be difficult to pinpoint because of the volume and complexity of the data. The following images demonstrate how you can view and filter data in the facet breakdown to quickly locate suspicious activity.

The following images were generated by creating an InstaQuery to search for connections to a specific IP address. The results of the query were visualized into a sunburst diagram with these facets: device, primary image path, destination port, and destination address.

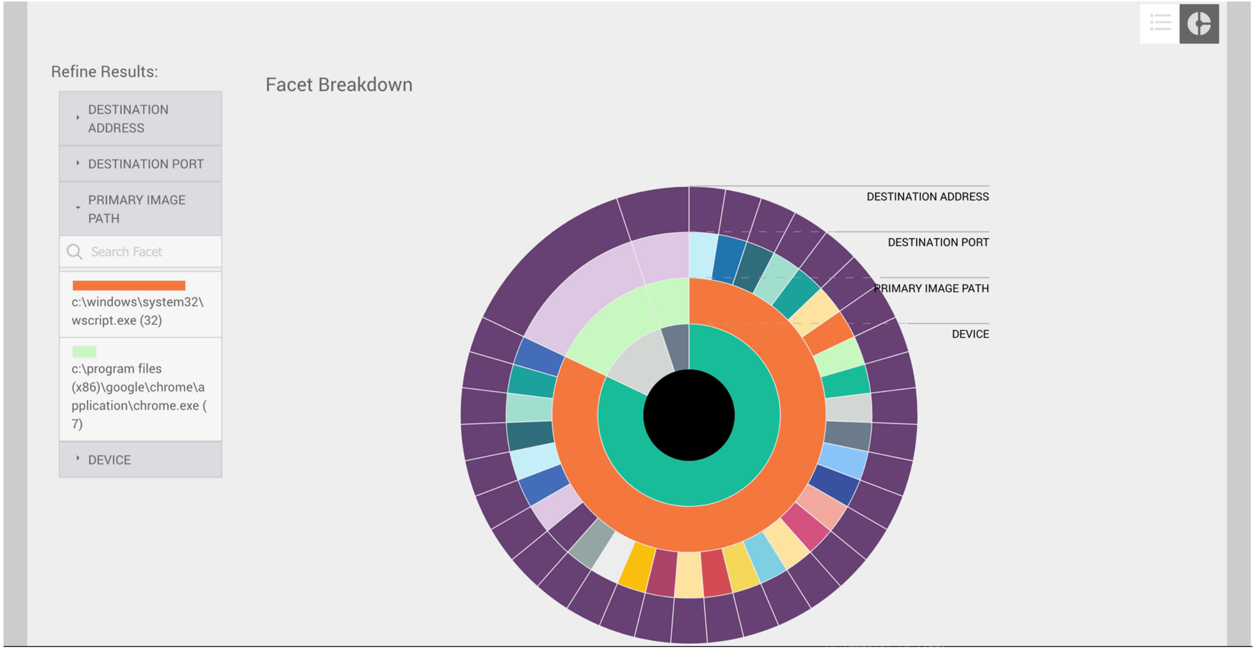


You can hover over any of the facets to display their associated values. In the following image, the administrator selected the outermost facet to view the name of the device, the path to the file that initiated the network connection, the port number used for the connection, and the IP address of the remote system.



When you hover over a facet, the associated parent facets are also highlighted to help you draw a visual relationship between the data points. In the example above, you can see that one device and one parent process were responsible for most connections to the IP address. The diagram also illustrates 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 in the diagram.

You can also obtain useful information from the refine results menus. Each of the facet menus contains the unique values and the number of occurrences for each facet. In the example below, you can see that there are two processes that were responsible for connections to this IP address: Google Chrome and Wscript.



When you click a facet value in the refine results menu, the diagram will change to display the facets that are directly related. This feature is useful to filter out irrelevant data and allow for a more focused analysis.

Create an advanced query

The advanced query feature allows you to build custom queries to enhance your threat hunting activities. Advanced query offers deep visibility into your CylanceOPTICS environment, expansive query options, and optimized workflows that allow you to combine related searches to reveal new insights. Advanced query is supported for devices with the CylanceOPTICS agent version 3.0 or later.

Advanced query relies on the use of EQL syntax. You use EQL to construct queries for events, and the results provide information about the artifacts that were involved in those events. The advanced query UI includes syntax information to help you build EQL queries.

Before you begin: Review Supported EQL syntax for advanced query and Sample CylanceOPTICS EQL queries.

1. In the management console, on the menu bar, click **CylanceOPTICS > Advanced Query**.
2. Do one of the following:

Task	Steps
Create a new advanced query	If you want to use an existing query template to create a new query, click **Show Template List** and click a template, then skip the first step below. **a.** In the query field, type or paste the EQL syntax for the query. As you type, syntax options and validation messages will display to help you build your query. If you want to save the current query as a template, click **Save As Template**. Type a name and description and select whether you want the template to be private or available to all administrators. Click **Save**. You can pin, edit, and delete queries from the templates list. **b.** To set the scope of the query, under **Search devices**, click **By Zone** or **By Device** (an icon next to each device indicates whether the device is online). Select one or more zones or devices, then click **Save**. If you don't set the scope, the query applies to all zones and devices. **c.** To set a date and time range for the query, click 📅 and configure the range. Click **Apply**. If you don't set a range, the query applies to all available data. **d.** Do one of the following: • If you want to run the query, click **Run Query**. • If you want to schedule the query to run at a specific date and time or on a regular interval, click **Schedule Query**. Type a name and description, select whether you want the query to be private or visible to all users, and set the date, time, and optional recurrence settings. If you want to restrict the query to the data that has been collected since the previous run, select the **Query only new data** check box. Click **Schedule Query**. On the **Scheduled Queries** tab you can view and edit scheduled queries and view and export the results. You can have a maximum of 25 queries that are actively running or scheduled to run. Stopped queries or single run queries that have completed do not count towards this limit. If you want to save query results to view them later from the **Query Snapshots** tab, in the results section, click 💾. Type a name and description and select whether you want the results to be private or visible to all users.
View a query snapshot	On the **Query Snapshots** tab, click a query snapshot. Note that this displays the original results of the query when it was saved and is not a new query.

3. If you want to filter the query results, do any of the following:

   - To filter query results by date and timestamp, click one or more bars of the histogram to filter by that date and time range. Click any bar in the selected range to remove the date and time filter.
   - To filter query results by a column, click ▽ for that column (for example, Device) and select the filter criteria.
   - To filter query results by a value that you specify, click 🔍 above the query results, then type or paste the value into the search field (for example, a specific timestamp, an event detail value, and so on).

4. Expand a result to display details. Click » to open a panel that includes event details and information about associated alerts (you may need to scroll to the right in the results window). To filter the query results to show the matches for one or more specific facets, click ▽ for those facets. Click the icon again to remove the filter.

5. In the query results, expand the ⋮ menu to view the available actions for each result. Depending on the type of result, this can include:

- Request and view focus data.
- Globally quarantine a file. The file appears in **Settings > Global List > Global Quarantine**, in **Protection > Threats**, and in the **Threats** section of the device details.
- Request and download a file. If path information is available for files associated with other artifact types, you can also download those files. The file is compressed and password-protected to ensure that it is not accidentally executed. The password is “infected". The size limit for file retrieval is 50 MB. Artifacts and files are retained by CylanceOPTICS for 30 days.

6. If you want to pin a result so that it displays with a visual marker if it shows up in subsequent queries, click 🔖.

After you finish:

- If you want to export the query results to a .csv file, click ⇥. Type a name and description, specify whether you want the exported results to be private or visible to all administrators, and click **Export**. You can download the file from the **Exported Results** tab when it is ready.
- To add a new query, click + next to the current query tab.
- To copy an existing query, hover over that query tab and click ⧉.

Supported EQL syntax for advanced query

Syntax help

The syntax help pane on CylanceOPTICS > Advanced Query lists the available CylanceOPTICS event classes and their associated artifacts, types, categories, and subcategories. As you type, syntax options and validation messages will display to help you build your query.

EQL query format

CylanceOPTICS EQL queries use the following format for a basic query:

```
<event class> where <event/artifact>.<facet> == <value>
```

A query searches for events that are related to artifacts, so you need to use the relevant event class in your query.

The where clause can filter the results based on the event.type, event.category, event.subcategory, or artifact.facet values.

You can use `or` or and to combine multiple filter clauses.

Match any event class

You can use `any` for the event class, which maps to all available event classes.

Escape an event class

To escape event classes that contain a special character (for example, a hyphen or period), contain a space, or start with a numeral, use enclosing quotation marks (") or three enclosing quotation marks (""").

Escape a field name

To escape field names that contain a hyphen, space, or start with a numeral, use enclosing backticks (`). Use double backticks (``) to escape any backticks (`) in the field name.

Escape a value

If you use a special character in a value, including a quotation mark or a backslash, it must be escaped with a preceding a backslash (for example, \” for a quotation mark, \\ for a backslash).

Conditions

A condition consists of one or more criteria that an event must match. You can specify and combine criteria with the operators described in the following sections.

Comparison operators

Operator	Description
<	This operator returns true if the value to the left of the operator is less than the value to the right. Otherwise, it returns false.
<=	This operator returns true if the value to the left of the operator is less than or equal to the value to the right. Otherwise, it returns false.
==	This operator returns true if the values to the left and right of the operator are equal. Otherwise, it returns false. Wildcards are not supported.
:	This operator returns true if strings to the left and right of the operator are equal. Otherwise, it returns false. Can be used to compare strings only.
!=	This operator returns true if the values to the left and right of the operator are not equal. Otherwise, it returns false. Wildcards are not supported.
>=	This operator returns true if the value to the left of the operator is greater than or equal to the value to the right. Otherwise, it returns false. When comparing strings, the operator uses a case-sensitive lexicographic order.
>	This operator returns true if the value to the left of the operator is greater than the value to the right. Otherwise, it returns false. When comparing strings, the operator uses a case-sensitive lexicographic order.

= is not supported as an equal operator. Use == or : instead.

Pattern comparison keywords

Operator	Description
like	This operator returns true if the string to the left of the keyword matches the string to the right (case-sensitive). It supports list lookups (see lookup operators below) and can be used to compare strings only. For case-insensitive matching, use like~.

Operator	Description
regex	This operator returns true if the string to the left of the keyword matches a regular expression to the right (see Regular expression syntax). It supports list lookups and can be used to compare strings only. For case-insensitive matching, use regex~.

```
my_field like  "VALUE*"         // case-sensitive wildcard matching
my_field like~ "value*"         // case-insensitive wildcard matching

my_field regex  "VALUE[^Z].?"   // case-sensitive regex matching
my_field regex~ "value[^z].?"   // case-insensitive regex matching
```

Limitations for comparisons

You can't chain comparisons. Use a logical operator between comparisons instead (see the logical operators section below).

For example, `foo < bar <= baz` is not supported but `foo < bar and bar <= baz` is supported.

You cannot compare a field to another field, even if the fields are changed using a function.

The following query is not valid because it compares the process.parent.name field value to the process.name field:

```
process where process.parent.name == "foo" and process.parent.name == process.name
```

The following query is valid because it compares both the process.parent.name and process.name fields to static values:

```
process where process.parent.name == "foo" and process.name == "foo"
```

Logical operators

Operator	Description
and	This operator returns true only if the condition to the left and right both return true. Otherwise, it returns false.
or	This operator returns true if one of the conditions to the left or right are true. Otherwise, it returns false.
not	This operator returns true if the condition to the right is false.

Lookup operators

Operator	Description
in	This operator returns true if the value is contained in the provided list (case-sensitive). For case-insensitive matching, use in~.

Operator	Description
not in	This operator returns true if the value is not contained in the provided list (case-sensitive). For case-insensitive matching, use not in~.
:	This operator returns true if the string is contained in the provided list. It can be used to compare strings only.
like	This operator returns true if the string matches a string in the provided list (case-sensitive). It can be used to compare strings only. For case-insensitive matching, use like~.
regex	This operator returns true if the string matches a regular expression pattern in the provided list (see Regular expression syntax). It can be used to compare strings only. For case-insensitive matching, use regex~.

```
my_field in ("Value-1", "VALUE2", "VAL3")                 // case-sensitive
my_field in~ ("value-1", "value2", "val3")                // case-insensitive

my_field not in ("Value-1", "VALUE2", "VAL3")             // case-sensitive
my_field not in~ ("value-1", "value2", "val3")            // case-insensitive

my_field : ("value-1", "value2", "val3")                  // case-insensitive

my_field like  ("Value-*", "VALUE2", "VAL?")              // case-sensitive
my_field like~ ("value-*", "value2", "val?")              // case-insensitive

my_field regex  ("[vV]alue-[0-9]", "VALUE[^2].?", "VAL3") // case-sensitive
my_field regex~  ("value-[0-9]", "value[^2].?", "val3")   // case-insensitive
```

Match any condition

Use the `where true` condition to match events solely on event category. For example, the following query matches any file events:

```
file where true
```

To match any event, you can combine the any keyword with the where true condition:

```
any where true
```

Query examples

See Sample CylanceOPTICS EQL queries.

Sample CylanceOPTICS EQL queries

Query DNS lookups for a specified URL:

```
network where dns.questions.question_name == "<URL>"
```

Query a specified WMI namespace:

```
application where event.subcategory == "wmi" and wmi_trace.namespace ==
 "<namespace>"
```

Query files with any of the specified SHA256 values:

```
file where file.sha256 in ("<value>", "<value>", "<value>")
```

Query processes with the specified process name:

```
process where process.name == "<name>"
```

Query processes where the command line contains a specified string:

```
process where process.command_line like "<string>"
```

Query information about network connections to a specified IP address on a specified port:

```
network where network.destination.ip_address == "<IP>" and
 network.destination.port == "<port>"
```

View focus data

Focus data allows you to visualize and analyze the chain of events, and the associated artifacts and facets of those events, that resulted in a piece of malware or another security threat on a device. Focus data is retained for 30 days.

For devices with CylanceOPTICS agent 2.x and earlier, the console can retrieve focus data only from devices that are online. For devices with agent 3.0 and later, devices do not need to be online because the console can retrieve the latest data available in the CylanceOPTICS cloud database.

Before you begin: If you want to enable the automatic upload of focus data for devices to the management console, turn on these options in the device policy. If you do not select this option, you must use the console to manually request focus data.

Do any of the following:

Task	Steps
View focus data from device details.	**a.** In the management console, on the menu bar, click **Assets > Devices**. **b.** Click a device and review the **Threats & Activities** section. **c.** If you did not enable the automatic upload of focus data, for a threat or event, click **Request Data**. **d.** Click **View Data**.
View focus data from an InstaQuery.	To create a new InstaQuery, see Create an InstaQuery. **a.** In the management console, on the menu bar, click **CylanceOPTICS > InstaQuery > Previous Queries**. **b.** For an InstaQuery, click **View Results**. **c.** For a result, click **Actions > Request Focus Data**. **d.** Click **View Focus Data**.

Task	Steps
View focus data from a master list.	**a.** In the management console, on the menu bar, click **CylanceOPTICS > Focus Data**. The list includes the focus data that was previously requested by an administrator or automatically uploaded to the console. **b.** For an artifact or event, click **View Focus**.

After you finish:

- Some artifacts or facets in the focus data may include a **Create InstaQuery** option to retrieve more information. This is known as a pivot query. The artifact or facet properties are prepopulated, you only need to specify the appropriate zones. The pivot query results are then available with the associated focus data.
- If you want to export focus data to a .csv file, click ▦, then click ⎘.

View and download files that CylanceOPTICS has retrieved

When CylanceOPTICS identifies a file as a potential threat, you can retrieve the file from the device (for example, when you review detection details or InstaQuery results). You can view a list of all of the files that CylanceOPTICS has retrieved, and you can download files from this view for further analysis.

1. In the management console, on the menu bar, click **CylanceOPTICS > Action History**.
2. lick the **File Download History** tab.
3. If you want to filter the results, click ≡ .
4. If you want to download a file, click **Download File**. Review the warning and click **Confirm Download**.

Using CylanceOPTICS to detect and respond to events

CylanceOPTICS uses the Context Analysis Engine (CAE) to analyze and correlate events as they occur on devices in near real-time. The CAE logic is stored locally on the device, which allows the CylanceOPTICS agent to monitor and track malicious or suspicious activity even if the device is not connected to the CylanceOPTICS cloud services. You can configure CylanceOPTICS to take automated response actions when the CAE identifies certain artifacts of interest, providing an additional layer of threat detection and prevention to complement the capabilities of CylancePROTECT Desktop.

You can customize the detection capabilities of CylanceOPTICS to suit the needs of your organization. You can create detection rule sets with your desired configuration of detection rules and responses, you can clone and modify existing detection rules or create your own custom rules, and you can create detection exceptions to exclude specific artifacts from detection.

Create a detection rule set

Create and apply a detection rule set to configure the types of events that you want CylanceOPTICS to detect and how you want CylanceOPTICS to respond to those events. A default detection rule set is available to help you test and evaluate how you want to use detection rules. In the default rule set, all detection rules are turned on and automated responses and user notifications are turned off.

When you create a detection rule set, it is a best practice initially to turn on the desired detection rules without response actions and desktop notifications. After you evaluate the detections data, you can configure the appropriate response actions and user notifications for each rule.

Before you begin:

- To view a rule set, you require an administrator role with the View ruleset and Edit ruleset permissions from the Endpoint Detection Response section.
- For more information about the optional CylanceOPTICS rules that you can import for your organization's environment, see KB76816.

1. In the management console, on the menu bar, click **CylanceOPTICS > Configurations**.
2. On the **Rule Sets** tab, click **Create New**.
3. Type a name and description.
4. If you want the CylanceOPTICS agent to display a message when a rule is triggered on the device, in the **Detection Notification Message** field, type the message.
5. Review the available rules. For each rule, you can hover over the information icon to view a description. Click **ON** to enable an entire rule group or a specific rule.
6. If you want to display a desktop notification when a rule is trigged on a device, select the **Display Detection Notification on Device** check box for the rule.
7. If you want the CylanceOPTICS agent to execute a response action when a rule is triggered on a device, in the **Response** drop-down list for the rule, select one or more actions. You can hover over the information icon for each action to view a description.
8. In the **Device Policy** drop-down list, click one or more device policies that you want to assign the detection rule set to.

   You can also assign a detection rule set to a device policy when you create or change a device policy.
9. Click **Confirm**. Review the summary then click **Confirm** again.

After you finish: After you assign the detection rule set to a device policy, you can view and manage detections. You can also do any of the following optional tasks:

- To reduce false positives or duplicate events, you can create detection exceptions.
- Create custom detection rules.
- Create a package playbook to respond to events.

Event responses

The CylanceOPTICS agent can execute the following response actions when a detection event is triggered:

Response	Description
Application Log	The agent logs detection events to the Windows application log.
Delete Files	The agent permanently deletes any file artifacts that are identified as an artifact of interest (AOI).
Delete Registry Keys	The agent permanently deletes the entire registry key of any AOI that are identified as registry artifacts.
Delete Registry Values	The agent permanently deletes the registry value of any AOI that are identified as registry artifacts.
Dump Detection to Disk	The agent creates a detection data file in the CylanceOPTICS application data directory.
Log Off All Users	The agent logs off all interactive and remote users.
Log Off Users	The agent logs off the specified users.
Log Off Interactive Users	The agent logs off all users that are currently physically interacting with the device.
Log Off Remote Users	The agent logs off all users that currently have a remote session established on the system.
Notification Window	The agent displays a notification window with the detection notification message that you specified, using the native OS notification box instead of the CylancePROTECT agent.
Suspend Processes	The agent suspends any process artifacts that are identified as an AOI.
Suspend Process Trees	The agent suspends the entire process tree of any process artifacts that are identified as an AOI. The AOI is treated as the root of the tree.
Terminate Processes	The agent terminates any process artifacts that are identified as an AOI.
Terminate Process Trees	The agent terminates the entire process tree of any process artifacts that are identified as an AOI. The AOI is treated as the root of the tree.
Whitelist Processes	This option excludes the specified processes from being observed by CylanceOPTICS.

View and manage detections

You can use the management console to view and analyze the events detected by the CAE. From the detections dashboard you can see trends in events over varying timeframes, the severity of different detections, and you can access detailed information for each detection.

Before you begin: Create a detection rule set.

1. In the management console, on the menu bar, click **CylanceOPTICS > Detections**.
2. Do any of the following:

Task	Steps
Change the scope of the detections data.	In the **Detections Over Time** drop-down list, select the desired scope.
Include or exclude detections of different priority levels.	The graph provides a count of informational, low, medium, and high priority events. Click any of the counts to exclude those events from the detections data. Click the same item again to include it in the data.
View the details and artifacts of interest for a detection.	Click **View**. Depending on the artifacts associated with the detection, you may be able to select different actions (for example, you can download a file, quarantine a file, view focus data, create a detection exception, and so on). You can click the **Detection Notes** section to add notes relevant to your analysis.
Lock down the device associated with a detection.	**a.** Click **View**. **b.** In the **Actions** drop-down list, click **Lockdown Device**. **c.** See Lock a device.
Export detection details to a JSON file.	**a.** Click **View**. **b.** In the **Actions** drop-down list, click **Export Data**.
Set the status of a detection event.	Do any of the following: • Click the **Status** drop-down list for a detection and select the appropriate status. If you select **False Positive**, you are prompted for how you want to handle duplicate detections. Select the appropriate option and click **Save**. • Select one or more detections and click **Select Action > Change Status**. Select the appropriate status and click **Confirm**.
Delete one or more detections.	Select the detections and click **Select Action > Delete Detection**. Click **Confirm Delete**.

Creating custom detection rules

To meet your organization's security needs and requirements, you can use the CylanceOPTICS rule editor to clone and modify the detection rules that are available in the management console, or you can create your own custom detection rules. You can use the flexibility and logic of the Context Analysis Engine (CAE) to detect suspicious or malicious activity, including monitoring for broad behavior characteristics (for example, files that use certain naming patterns) or a targeted series of events (for example, a process with a certain file signature thumbprint that creates files and initiates network connections). Custom detection rules use the same workflow as the detection rules offered by BlackBerry, and you can configure automated response actions, user notifications, and package playbooks for your custom rules.

The rule editor uses JSON and provides built-in validation tools. When you validate a rule, the editor will check the syntax to identify any issues. If the rule passes the syntax check, CylanceOPTICS will then use a CAE service to verify that the rule will compile and run on a device. If either validation process discovers an issue, it will provide information about the errors that you must correct. After a rule passes both validation checks, you can publish the rule and add it to detection rule sets.

This section provides guidance and reference information for building your own CAE rules. CAE rules support the following data and filters:

Item	Description
States	States define the flow of a CAE rule, allowing CylanceOPTICS to statefully observe a series of events that can occur on a device. States represent a "1, then 2, then 3" scenario that might occur.
Functions	Functions define the logic that is required to successfully fulfill a state. This logic applies directly to the defined field operators and represents the attributes of an event that occurs on a device (for example, “A, and B, and C” or “A, and B, but not C”).
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 are the values that CylanceOPTICS compares. Operands allow for the extraction of specific pieces of data about an event (for example, file paths, file hashes, and process names) and compares those with literal values (for example, string, decimal, boolean, and integer).
Artifacts of interest	Artifacts of interest define the artifacts that CylanceOPTICS can target when it executes automated response actions (for example, terminating processes, logging off users, or deleting files).
Paths	Paths define how the CAE interprets the flow of multiple state objects within a rule.
Filters	Filters narrow or expand the scope of a state with a smaller or larger number of events to analyze.

To address performance issues in environments that generate abnormally high numbers of events (for example, server systems or software engineering systems), the CAE supports exclusion rules that you can use to exclude certain events from the CylanceOPTICS data pipeline. CylanceOPTICS does not analyze or record excluded events. You can use preconfigured exclusion rules that are available in the management console, or you can use the rule editor to create your own exclusion rules using the same JSON structure as detection rules. The goal of an exclusion rule is to satisfy the rule based on processes that you want to exclude.

After you publish an exclusion rule, you can associate it with the whitelist process response action in a detection rule set. With this response action, the CAE will automatically exclude any events and processes that match the associated rule logic. Use caution when you use exclusion rules, because they have the potential to reduce the overall security of CylanceOPTICS devices.

Sample detection rule

See the following topics to understand the format and options for CAE rules:

- States
- Functions
- Field operators
- Operands (facet value extractors)
- Artifacts of interest
- Paths
- Filters

```
{
    "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"
    ]
}
```

To review another example of a custom detection rule, see KB66651.

Create and manage detection rules and exclusions

Before you begin: If you want to clone and modify an existing detection rule, or create your own custom rule, review the following topics and the sample detection rule to understand the format and options for CAE rules:

- States
- Functions
- Field operators
- Operands (facet value extractors)
- Artifacts of interest
- Paths
- Filters

1. In the management console, on the menu, click **CylanceOPTICS > Configurations**, then click the **Rules** tab.

   You can sort and filter the available detection rules and view information for each rule.
2. Do any of the following:

Task	Steps
Export a rule to a .json file.	You can export detection rules from any of the following rule categories: Custom, Cylance Experimental, Cylance Exclusion, Cylance macOS Official, Cylance Windows Official. Click ⇥ for a rule.
Import a custom detection rule from a .json file.	**a.** Click **Import Rule**. **b.** Browse to and select or drag and drop the .json file. Click **Import**. **c.** Change the rule configuration and syntax as required. **d.** Click **Validate**. **e.** Click **Publish**. To edit a custom rule after it has been published, click ✎ for the rule.

Task	Steps
Clone and modify a detection rule.	You can clone detection rules from any of the following rule categories: Custom, Cylance Experimental, Cylance Exclusion, Cylance macOS Official, Cylance Windows Official. **a.** Click ⧉ for a rule. **b.** Change the rule configuration and syntax as required. **c.** Click **Validate**. **d.** Click **Publish**.
Delete a custom rule.	You can delete rules from the Custom category only. **a.** Click 🗑 for a rule. **b.** Click **Confirm Delete**.

States

States are the highest logic level of a CAE rule and have a larger number of required fields.

Field name	Description
Actions	This field contains a list of the objects that are used to define artifacts of interest within a state. For more information, see Artifacts of interest.
ActivationTimeLimit	This field defines how long CylanceOPTICS will wait for events to trigger the event. The recommended default value is -0:00:00:001.
FieldOperators	This field contains the field operators and operands that should be inspected to fulfill the function that is defined in the state. For more information, see Field operators.
Filters	This field defines which event categories, subcategories, and types that CylanceOPTICS should inspect when trying to fulfill a state. For more information, see Filters.
Function	This field contains the logic function that CylanceOPTICS must observe to consider a state to be satisfied. For more information, see Functions.
HarvestContributingEvents	This field defines whether CylanceOPTICS should record the events that satisfy a state. The recommended value is true.
Name	This field defines the name of the state that will be displayed in the UI if the rule is satisfied.
Scope	This field defines the scope in which CylanceOPTICS looks for relevant events. In most cases, the recommended value is global.
States	This field contains a list of one or more state objects. These objects can be chained.

Functions

Functions define the logic that is required to fulfill a state for a CAE rule. This logic applies directly to the defined field operators and is used to represent "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 satisfy the state.	a & b & c
OR - |	One of two or more field operators must be matched to satisfy the state.	a | b | c
NOT - !	A defined field operator must be false or not matched to satisfy the state.	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 considers that portion of the defined function to be complete. When all pieces of the function are complete, the state is satisfied.

The field operators field is an object that consists 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. BlackBerry recommends that these names are kept to simple and logical values, such as numbers or letters.

Field operator	Description
Base64Encoding Base64	This field operator tokenizes a string and determines if any of the tokens match an operand. It also attempts to determine the type of string encoding (ASCII, UTF-7, UTF-8, UTF-16-LE, UTF-16-BE, UTF-32-LE, or UTF-32-BE). Without a BOM, the operator can reliably detect only UTF-8, UTF-16-LE, and UTF-16-BE. If all detections fail, the operator will default to the system's default code page. Postive: `powershell.exe -ex bypass -e "ZwBlAHQALQBwAHIAbwBjAGUAcwBzAA==" equals ("get-process", )` Negative: `powershell.exe -ex bypass "ZwBlAHQALQBhAGwAaQBhAHMA" does not contain ("get-process", )`
ContainsAll	This field operator 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")

Field operator	Description
ContainsAllWords	This field operator 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 or 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")
ContainsAny Contains	This field operator 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")
ContainsAnyWord ContainsWord	This field operator 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 or 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")
DamerauLevenshteinDistance DLDistance	This field operator determines if the distance (the number of changes needed to turn one operand into another operand) is within an acceptable range, but allows for the transposition of adjacent symbols. Positive: "cat" is within a Damerau-Levenshtein Distance of 1 from "bat" Positive: "hello" is within a Damerau-Levenshtein Distance of 2 from "bell" Positive: "ca" is within a Damerau-Levenshtein Distance of 3 from "abc" Negative: "cart" is not within a Damerau-Levenshtein Distance of 1 from "act"

Field operator	Description
DiceCoefficient Dice	This field operator determines the similarity between two sets or strings by the number of common bigrams (a pair of adjacent letters in the string). It determines if the result of the comparison falls between the "mincoefficient" and "maxcoefficient". For example, comparing the process name "Test.exe" with "Tes.exe" would return 0.76923076923076927. With "round" set to 2: Positive: min: 0.5 < 0.77 < 0.8 max; not inclusive Positive: min: 0.77 <= 0.77 <= 0.77 max; inclusive Negative: min: 0.8 < 0.77 < 0.85 max; not inclusive The "round" option will round the decimal place to the specified integer. For example, if "round" is set to 2, .6666666667 becomes .67.
EndsWithAny EndsWith	This field operator 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"
EqualsAny Equals	This field operator 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 or 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	This field operator 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
GreaterThanOrEquals	This field operator 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

Field operator	Description
HammingDistance	This field operator determines the distance between two strings of equal length, which is the number of positions at which the corresponding symbols are different. It measures the minimum number of substitutions required to change one string into the other. Positive: "cat" is within a Hamming Distance of 1 from "bat" • cat → bat(1) Positive: "hello" is within a Hamming Distance of 2 from "bell" • hello → bello(1) → bell(2) Positive: "ca" is within a Hamming Distance of 3 from "abc" • ca → aa(1) → ab(2) → abc(3) Negative: "cart" is not within a Hamming Distance of 4 from "act" • cart → aart(1) → acrt(2) → actt(3) → act(4)
HexEncoding	This field operator tokenizes a string and determines if any of the tokens match an operand. It also attempts to determine the type of string encoding (ASCII, UTF-7, UTF-8, UTF-16-LE, UTF-16-BE, UTF-32-LE, UTF-32-BE). Without a BOM, it can reliably detect only UTF-8, UTF-16-LE, and UTF-16-BE. If all detections fail, the operand will default to the system's default code page. Positive: "74657374" contains "test" Negative: "696e76616c6964" does not contain "test"
InRange	This field operator 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
IpRange</td><td>
This field operator determines if the TargetNetworkConnection address (SourceAddress, DestinationAddress) is within the specified "min" and "max" options.

Allowed Operands are:

<pre>
{
    "Source": "TargetNetworkConnection",
    "Data": "SourceAddress"
}
</pre>

And:

<pre>
{
    "Source": "TargetNetworkConnection",
    "Data": "DestinationAddress"
}
</pre>

Example:

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

Include the following filters object with the above example to output the network traffic:

<pre>
"Filters": [
    {
        "Type": "Event",
        "Data": {
            "Category": "Network",
            "SubCategory": "*",
            "Type": "Connect"
        }
    }
]
</pre>
</td></tr>
</table>

Field operator	Description
IsFlagSet	This field operator checks if a bit or bits in a bitmask are set. It can use base-10 or base-16 (using the "0x" prefix) for the comparison value. Positive: 0x10 is set for 0x4111 Positive: 3 is set for 0x7 Negative: 0x3 is not set for 0x4 Negative: 2 is not set for 0x5
IsHomoglyph	This field operator determines if the left operand is a homoglyph of the right operand. For example, a US Latin 1 "e" and a French "e" appear to be the same character and have the same meaning, but they have 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	This field operator 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 Exists HasContent	This field operator 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	This field operator determines if the specified value is true. Positive: TriState.True Negative: TriState.False Negative: TriState.Unknown
LessThan	This field operator 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

Field operator	Description
LessThanOrEquals	This field operator 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
LevenshteinDistance	This field operator 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"
LongestCommonSubsequence	This field operator compares a fixed left operand with a set of right operands and determines the longest subsequence in each comparison. It compares the result count to min and max values to determine if the result is within an acceptable range. Comparing "aggtab" and "gxtxayb": Positive: "gtab" is the longest sequence. If the min is 1 and max is 10, this falls within an acceptable range. Negative: Using the previous example, if the min was 5 and the max was 10, this would not fall within an acceptable range.
LongestCommonSubstring	This field operator compares the left and right operands and returns a count of the longest found substring. Comparing "ababc" and "abcdaba": Positive: "aba" and "abc" are two results of the same size in "abcdaba" and would return the longest substring as 3. Negative: If the mindistance and the maxdistance was set to 4, this would be larger than the longest substring found. Comparing "ababcd" and "abcdaba": Postive: "abcd" is the longest substring found.
MatchOnFilter NoOp	This field operator indicates that no operations are being performed and that the state simply matches if the filter finds a corresponding event.
RegexMatches	This field operator determines if the specified operand conforms to a regular expression. Positive: "hello, I am a string" conforms to "^hello, [Ii] am [aA] string$" Negative: "hello, I am a string" does not conform to "^[hi\|hey], I am a string$"

Field operator	Description
ShannonEntropy	This field operator determines the measure of unpredictability of state, or its average information content when comparing a single operand. Postive: "abc" calculates to 1.5849625007211561 and falls within the range of 1.55 and 1.6. Negative: "Z2V0LXByb2Nlc3M=" calculates to 3.875 and does not fall within the range of 1.55 and 1.6.
StartsWithAny StartsWith	This field operator 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)

The CylanceOPTICS CAE uses facet value extractors to identify an individual property (facet) of a single artifact that is associated with an event that CylanceOPTICS observed. 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 to trigger a detection event.

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

Extractor name	Description	Supported facets
InstigatingProcessImageFile	This extractor extracts a facet from the image file that is associated with the instigating process of an event. It is commonly used to inspect various attributes of the image file (for example, name, path, hash, 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) LeafSignatureAlgorith (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	This extractor extracts a facet from the owner associated with the instigating process of an event. It is commonly used to inspect the user who owns the process.	Name (as String) Domain (as String)

Extractor name	Description	Supported facets
TargetFile	This extractor extracts a facet from a file on which an event occurred. It is commonly used to inspect various attributes of the file (for example, name, path, hash, or signature status).	See InstigatingProcessImageFile above.
TargetFileOwner	This extractor extracts a facet from the owner that is associated with the file on which an event occurred. It is commonly used to inspect the user who owns the file.	See InstigatingProcessOwner above.
TargetNetworkConnection	This extractor extracts a facet from the network connection on which an event occurred. It is commonly used to inspect the network IP address or the port that is acted on.	SourceAddress (as IPAddress) SourcePort (as Integer) DestinationAddress (as IPAddress) DestinationPort (as Integer)
TargetProcess	This extractor extracts a facet from the process on which an event occurred. It is commonly used to inspect the name or command line arguments of a process that is acted on.	See InstigatingProcess above.
TargetProcessImageFile	This extractor extracts a facet from the image file that is associated with a process on which an event occurred. It is commonly used to inspect the attributes of the image file (for example, name, path, hash, or signature status).	See InstigatingProcessImageFile above.

Extractor name	Description	Supported facets
TargetProcessOwner	This extractor extracts a facet from the owner that is associated with a process on which an event occurred. It is commonly used to inspect the user who owns the process that is acted on.	See InstigatingProcessOwner above.
TargetRegistryKey	This extractor extracts a facet from the registry key on which an event occurred. It is commonly used to inspect the registry key or value that is acted on.	Path (as String) ValueName (as String)

Path value extractors

Extractor name	Description
EnvVar	EnvVar extracts an environment variable from the OS.
LiteralWithEnvVar	LiteralWithEnvVar expands a path that contains an environment variable.
Literal	Literal represents a literal value and is the most common extractor and operand.

Artifacts of interest

You can use the artifacts of interest (AOI) in the actions field to define a list of artifacts that CylanceOPTICS can perform automated response actions on. The AOI follow the same syntax as operands. Any artifact that is 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.

If a filter is applied to a state, note 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, file and process related AOI would be available but would not have registry or network-related AOI. If 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

Category	Subcategory	Type	Applicable AOI
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
Network	UDP	Connect	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetNetworkConnection

Category	Subcategory	Type	Applicable AOI
Process	—	Exit	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetProcess TargetProcessImageFile TargetProcessOwner
Process	—	Start	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetProcess TargetProcessImageFile TargetProcessOwner
Process	CylancePROTECT Desktop	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
Registry	—	PersistencePoint: KeyDeleted	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetRegistryKey

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

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

Example:

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

Paths

Paths define how the CAE interprets the flow of multiple state objects within a rule. You use paths when a rule consists of multiple state objects (also known as a multistate rule). States define the flow of a CAE rule and 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.

If a rule has one state object only, you don't need to use a paths object. Rules consist of a single state object and do not explicitly require the use of the paths object. Rules that do utilize the paths object do so for explicit definition only (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. When 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

You can use filters to narrow or expand the scope of a state to account for a smaller or larger number of events to analyze. Event filters use the same event categories, subcategories, and types that are outlined in Data structures that CylanceOPTICS uses to identify threats.

Example 1: The following example limits inspected events to process start events.

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

Example 2: The following example inspects all types of file events (create, write, delete).

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

Create a detection exception

To reduce false positives or duplicate events in your detection results, you can create exceptions for detection rules. When you create a detection exception, the specified processes will not be evaluated by the CylanceOPTICS detection engine. Use caution when you create detection exceptions, because they have the potential to reduce the overall security of devices.

Note: If you create and enable a rule exception that uses only RegEx matches for conditions, it may cause higher than normal CPU usage on some systems with a consistently high number of events, due to the rule exception running on every event. If you encounter this issue, BlackBerry recommends disabling the rule exception that uses RegEx matches for conditions.

1. In the management console, on the menu bar, click **CylanceOPTICS > Configurations**.
2. On the **Exceptions** tab, click **Create Exception**.
3. Type a name for the detection exception.
4. In the **Conditions** section, configure exception conditions. Click **Add Another Condition** to configure additional exceptions.

   In a detection exception, an AND statement is applied to all conditions. All conditions must be met for the exception to be true. When you specify a value for a condition, it is treated as an ANY statement. When two or more values are added, if any of the values exist, the condition is true.
5. Click **Save**.

After you finish: On the menu bar, click **CylanceOPTICS > Configurations**, then click the **Rule Sets** tab. Edit a detection rule set and assign the detection exception to the desired rules. Click **Confirm**.

Deploy a package to collect data from devices

You can use the CylanceOPTICS package deploy feature to remotely and securely run a process (for example, a Python script) on CylanceOPTICS 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 CylanceOPTICS 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 > Packages**, then click **Upload file**.

1. In the management console, on the menu bar, click **CylanceOPTICS > Packages**.
2. Click **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 CylanceOPTICS 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**.

Create a package playbook to respond to events

When a security incident occurs on a device, you can minimize your response time by creating a package playbook. A package playbook allows you to automate the execution of refract packages when an event triggers a Context Analysis Engine (CAE) rule that you have configured in a detection rule set.

Package playbooks support Python refract packages only. You can use out-of-the-box refract packages that are available in the management console, or you can add your own custom refract packages. The contents of a package playbook are stored on the device, so they can be executed even if the device is offline. You can create a maximum of 100 package playbooks.

Before you begin:

- Create a detection rule set.
- If desired, create a Python refract package that can execute on a device when a detection rule is triggered. For more information about creating a custom package, see KB 66563.
- If you create your own package, you must upload it to the management console. In the console, go to **CylanceOPTICS > Configurations > Packages**, then click **Upload file**.

1. In the management console, on the menu bar, click **CylanceOPTICS > Configurations**, then click the **Playbooks** tab.
2. Click **Create Playbook**.

    If you want to clone an existing package playbook, filer the list of playbooks to the desired playbook and click ⧉.
3. Type a name and description.
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. In the **Package** drop-down list, click a package that you want to include in the package playbook. If necessary, specify optional command line arguments.
7. Click **Add Another Package** to add additional packages. You can add a maximum of 20 packages to a package playbook.
8. Click **Save**.

After you finish: On the menu bar, click **CylanceOPTICS > Configurations > Rule Sets**. Edit a detection rule set and assign the package playbook to the desired rules. Click **Confirm**. You can associate up to 10 package playbooks to each detection rule.

Lock a device

You can lock an infected or potentially infected device to stop command and control activity, the exfiltration of data, and the lateral movement of malware. You have the following lockdown options:

Lockdown type	Description
Full lockdown (all platforms)	Prevent all network communication from the device. You can lock a device for up to 96 hours. You can use an unlock key to unlock the device before the end of the lockdown period.
Partial lockdown (CylanceOPTICS agent 3.1 or later for Windows only)	Disable the device's LAN and Wi-Fi network capabilities and retain communication with the CylanceOPTICS cloud services, allowing CylanceOPTICS to continue to receive detections and sensor data. Partial lockdown persists indefinitely. You can unlock the device at any time using an unlock key or the remote unlock feature.
Customized partial lockdown (CylanceOPTICS agent 3.2.1140 or later for Windows only)	This option is the same as partial lockdown but also allows you to specify additional communication channels that you want to allow during a partial lockdown.

Before you begin:

- For the requirements to support the lockdown feature for Linux, see the CylanceOPTICS requirements.
- If you want to use a customized partial lockdown, on the menu bar, click **Settings > Detection and Response > Add New Configuration**. Specify a name, description, and the IP address, port, and operations (inbound, outbound, bidirectional) for the communication channels that you want to allow during partial lockdown. Click **Save**.

1. In the management console, on the menu bar, click **CylanceOPTICS > Devices**.
2. Click the device name.
3. Do one of the following:

Task	Steps
Fully lock a device (all platforms)	**a.** In the **Select Action** drop-down list, click **Lockdown**. **b.** If it is a Windows device, in the drop-down list, click **Full lockdown**. **c.** Select a lockdown period. **d.** Click **Confirm Lockdown**.
Partially lock a device (CylanceOPTICS agent 3.1 or later for Windows only)	**a.** In the **Select Action** drop-down list, click **Lockdown**. **b.** In the drop-down list, do one of the following: • To use the default partial lockdown configuration, click **Partial lockdown**. • To use one of your custom partial lockdown configurations, click the configuration. **c.** If you want to allow remote response sessions to the device while it is in a partial lockdown state, turn on **Remote Response**. **d.** Click **Confirm Lockdown**. To remotely unlock the device, click the device and in the **Select Action** drop-down list, click **Unlock device**. Confirm the remote unlock.

4. If you want to manually unlock a fully or partially locked device, click **Actions > Show Unlock Key**. Copy the unique unlock key and run the following commands on the device:

OS	Commands
Windows	**a.** Navigate to the CylanceOPTICS executable folder (by default, C:\Program Files\Cylance\Optics). **b.** Run `CyOptics.exe control --password "<unlock_key>" unlock -a`
macOS	**a.** Run `cd /Library/Application\ Support/Cylance/Optics/CyOptics.app/Contents/Resources` **b.** Run `sudo ../MacOS/CyOptics control --password <unlock_key> unlock -net`
Linux	Run `./CyOptics control --password "password" unlock -net`

Sending actions to a device

You can use the remote response feature to securely execute scripts and run commands on any CylanceOPTICS-enabled device directly from the management console, using a familiar command line interface.

When you start a remote response session, the CylanceOPTICS agent creates an instance of the device's native shell (cmd for Windows, bash for macOS and Linux) and handles the transfer of commands to and from the shell. As a result, you have access to the functions of the native shell and the apps and scripts that are available on the device. CylanceOPTICS also provides some reserved commands that you can use to transfer files to and from the device.

A remote response session can be initiated only with a device that is online and will time out after 25 minutes of inactivity. Multiple sessions can be open for the same device at the same time, to a maximum of 50.

Remote response provides a high level of access to a device, so use caution when you issue commands and comply with your organization’s security policies. When you use remote response, the details of the session, including the commands that are sent, information about file transfers, and the responses that are received, are recorded in the device log that you can access from the management console. The log file is retained for 30 days.

Start a remote response session

1. In the management console, on the menu bar, click **CylanceOPTICS > Devices**.
2. Find the device and click the device name.
3. In the **Select Action** drop-down list, click **Remote Response**.
4. Enter commands in the remote response session window.

   For more information about reserved commands for CylanceOPTICS, see Reserved commands for remote response.

After you finish: If you want to download the device log with the record of the remote response session, on the menu bar, click **CylanceOPTICS > Action History**. Find the device and click **Download Log**.

Reserved commands for remote response

The following reserved commands, which are common across the supported OS platforms, do not interact directly with the native shell on the device.

Item	Description
`rr-clear`	This command clears the remote response terminal window.
`rr-get <absolute_path_to_file>`	This command copies the specified file (which must include the file name) from the device and uploads it to your web browser so you can save it to your local system. If the file is larger than 70 MB, the command will fail with an error. Example: `rr-get C:\Program Files\Cylance\Desktop \2021-03-26.log`
`rr-help`	This command displays a list of the reserved commands.
`rr-put <destination_directory>`	This command opens a file browser window that allows you to select a file from your local system that will be sent to the specified directory on the device (for example, the user’s downloads folder). If the file is larger than 70 MB, the command will fail with an error. Example: `rr-put C:\Users\username\Downloads`
`rr-quit`	This command ends the remote response session. The terminal window remains open so you can view the session history, but commands are no longer sent or received.

Monitoring network connections with CylanceGATEWAY

You can monitor activity and events associated with users' network connections. CylanceGATEWAY logs all network activity for every user who has CylanceGATEWAY work mode enabled on their device. By default, the CylanceGATEWAY network activity data is retained for 30 days. You can search 30 days of logged network events.

Note: If CylanceGATEWAY is not enabled for your tenant, the menu options to configure it are not displayed in the management console.

Viewing network activity

CylanceGATEWAY logs all network activity for devices that have Work Mode and Safe Mode enabled. The network activity log records the user, device model and OS, hostname, destination, date and time, and other details about each attempted connection event. If Traffic privacy is enabled in an ACL rule, the network access attempts that the rule applies to are not logged on the Network Events screen or sent to the SIEM solution or syslog server, if configured.

If a connection is identified as a potential threat, the **Detections** column specifies the type of threat detected.

- **DNS Tunneling** detections are potential threats based on analysis of the DNS traffic from the client to the attacker's DNS server (for example, when a host is infected, the malware can initiate a command and control (C2) channel with its creator to attempt to exfiltrate data).
- **Reputation** detections are potential threats from addresses on the BlackBerry list of unsafe Internet destinations and are detected by destination reputation. Each destination is assigned a risk score. You can configure the risk level of the destination reputations to block.
- **Signature detection** detections refer to potential threats detected by signature detections. Signature-based detection is a methodology used to detect known malware that are stored as a part of a database. When a new malware signature is identified, cybersecurity experts will add the signature to a database.
- **Zero Day Detection** detections refer to newly identified malicious destinations (for example, domain generation algorithm (DGA) and phishing) that have not been identified previously. After they are identified, these destinations are assigned a risk score. They are subsequently blocked or alerted upon based on the risk level that you set for your network protection. For more information, see Configure network protection settings in the Cylance Endpoint Security Setup content.

To view the network activity log in the management console, on the menu bar, click **CylanceGATEWAY > Events**.

To view the details of a network event, click the activity log row. For more information on the event details, see Viewing the Event Details page.

To filter any column, click ≡ at the top of the column.

To perform a free form search, click 🔍 and type the search query. As you type the characters in the search field, you can select from the displayed matching options.

To change which columns are displayed, click ||| at the right side of the column headings.

To change the order of events columns, drag the column to where you want it to appear.

To export the network activity information to a .csv file, click ⇥. Select to export everything or only the filtered network activity and click **Export**.

To see how CylanceGATEWAY might classify a network destination that a user tries to access, see Evaluate the risk level of a network destination.

Viewing the Event Details page

You can view additional metadata and details for a network event that has been logged on the Events page. The metadata displayed depends on several factors such as the type of network request that is made and how you configured the ACL rules. For example, DNS events display DNS specific details and TLS events display TLS specific details. Similarly, if network protection is enabled in an ACL rule, additional metadata is displayed. You can share the network event with other console users to audit or investigate the destinations that the user has tried to access. Console users must have the appropriate permissions to view the shared event. Click < to copy the link to the event.

You can filter the logged network events using the following data filters:

Filter	Description
Event Overview	
Event ID	This is a unique identifier for the network event for your tenant.
Source IP	This is the private Gateway IP that was assigned to the endpoint tunnel during the event.
Source port	This is the port number of the destination.
DNS Query Name	This is the Resource Requested (RR) name of the DNS server that the CylanceGATEWAY agent queried.
DNS Query Type	This is the type of DNS query (for example, A, AAAA, or SRV record) that was sent to the DNS server.
Destination	This is the destination of the event. The destination IP address is always included. The event may also show the network service name, or hostname if applicable.
Destination port	This is the port of the destination that was being accessed.
Private NAT Source IP	This is the source IP address of this event as it left the CylanceGATEWAY Connector for one of your private networks. If the source IP is not available or the feature has not been enabled, the filter displays "Unknown". **Important:** You must ensure the CylanceGATEWAY Connector system time is accurate. If the CylanceGATEWAY Connector system time does not maintain an accurate system time, the NAT details reported by the connector might not be matched with the network event within the BlackBerry Infrastructure. By default, the CylanceGATEWAY Connector uses Ubuntu's timeserver (ntp.ubuntu.com server) for time synchronization or you can specify a custom NTP server. If you use Ubuntu time-server make sure that it can be accessed from your private network. For more information, see Configure the CylanceGATEWAY Connector. The CylanceGATEWAY Connector sends the updated NAT details to the Event Details screen every minute. This feature is enabled by default. If the Private NAT Source details are not displayed in the Event Details page in the Cylance console, ensure that you have installed the latest CylanceGATEWAY Connector and restarted the connector.

Filter	Description
Private NAT Source Port	This is the source IP port of this event as it left the CylanceGATEWAY Connector for one of your private networks. If the port number is not available or the feature has not been enabled, the filter displays "Unknown". This feature is enabled by default. If the Private NAT Source details are not displayed in the Event Details page in the Cylance console, ensure that you have installed the latest CylanceGATEWAY Connector and restarted the connector.
BlackBerry source IP	This is the IP address of this event as it left the BlackBerry Infrastructure. This BlackBerry source IP is not available for flows that do not use the CylanceGATEWAY tunnel (for example, Safe Mode).
Tunnel source IP	This is the IP address of the endpoint as seen by the BlackBerry Infrastructure when it comes to the CylanceGATEWAY tunnel.
Protocol	This is the protocol (Layer 4) that the network event used to access the destination. The protocol can be UDP or TCP.
App protocol	This is the protocol (Layer 6 or 7), such as TLS, DNS, or HTTP that was used for the communication.
Access Type	This is the access type (for example, Safe Mode or the Gateway tunnel) that the network event used to access the destination.
Network Route	This provides the traffic as public or private connections that were used to route traffic. For private connections, you can filter by the connector group name and each CylanceGATEWAY Connector.
Connector	This is CylanceGATEWAY Connector that the network event is associated with. To view more information about the connector, click the connector name.
Category	This is the category that is applied to the event. For example, if CylanceGATEWAY has identified the destination as containing possibly malicious threats, the category might display Dynamic Risk. For more information on the Dynamic Risk category, see Configuring network protection in the Setup content. The destination might also be categorized based on the content it contains such as "Computer and Information Technology". For more information on categories for destination content, see Destination content categories in the Setup content.
Subcategory	This is the network traffic subcategory description for the category that is associated with the destination. For more information on the subcategories that might be displayed if the category is Dynamic Risk, see Configuring network protection in the Setup content. For more information on the subcategories that might be displayed for if the category is a destination content category, see Destination content categories in the Setup content.
Start time (UTC)	This is the time when the network activity communication started. The time is displayed in UTC.
End time (UTC)	This is the time when the network activity communication ended. The time is displayed in UTC.

Filter	Description
PID	This is the numerical process ID of the process that initiated the DNS request. The PID is reported by the Windows or macOS device when the agent is enabled with Safe Mode.
Pathname	This is the path to the executable that the process was executed from. This is commonly displayed as the path to the svchost.exe. The path is truncated to 1024 characters. The path is reported by the Windows or macOS device when enabled with Safe Mode.
Transferred	This provides how many bytes were exchanged between the destination and the CylanceGATEWAY agent. This is displayed as the total bytes uploaded and downloaded to the server and CylanceGATEWAY agent.
Packet flow	This is the number of packets that were sent between the destination and the CylanceGATEWAY agent.
User	This is the username that the network event is associated with. You can filter the network events by a user's Active Directory username and display name. When you export the Events page, only the username is exported. You can click the username to view the events that are associated with the user.
OS	This is the device that was used to initiate the network activity (for example, Android, iOS, macOS, or Windows).
Model	This is the model of the device (for example, iPhone, Samsung Galaxy, Google Pixel).
Device	This is the host name of the user's macOS or Windows device (for example, example.com).
Action	This identifies whether the network event is allowed or blocked based on your network protection settings and the ACL rules that you have specified for the environment. Additional information for the action is included in the Action section.
Action	
Connection phase	This is the evaluation phase when the access attempt properties were compared against the destinations and conditions of each ACL rule. One or more of the phases (for example, during DNS lookup, connection attempt, and TLS handshake) which were evaluated against the ACL rules is displayed.
Time (UTC)	This is the time when the network activity was evaluated with an ACL rule. The time is displayed in UTC.
Applied rule	This is the name of the ACL rule that was applied at the time of the evaluation during the various phases of the ACL rules.
Action	This displays whether the action was allowed or blocked for evaluated phases.
Alerts	

Filter	Description
Type	This identifies the anomaly that was triggered by the network activity with the associated network protection level that is specified. For more information on the supported anomalies, see Viewing network activity.
Time (UTC)	This is the time that the network activity triggered the alert. The time is displayed in UTC.
Category	This is the anomaly that triggered the alert. For more information on anomalies, see Viewing network activity.
Signature	This is the signature anomaly that was triggered by the network event.
Transferred	
Downloaded	This is the total bytes of data that were sent from the destination to the CylanceGATEWAY agent.
Uploaded	This is the total bytes of data that were sent from the server destination to the CylanceGATEWAY agent.
TLS	
TLS version	This is the version of the TLS protocol that was used to connect to the destination.
Client ALPN	This is the ALPN header information that was sent to the CylanceGATEWAY agent from the destination.
Server ALPN	This is the header information that was sent from the destination to the CylanceGATEWAY agent.
SNI	This is the host name of the destination that the CylanceGATEWAY agent attempted to connect to.
Issuer	This is the certificate presented by the destination.
Subject	This is the name of the rule that was applied at the time of the evaluation during the various phases (for example, DNS lookup, connection establishment, and TLS handshake) in relation to the ACL rules.
Not valid before	This is the date before which the certificate is not valid.
Not valid after	This is the date after which the certificate is not valid.

Filter	Description
HTTP Events	This reports the original plain-text, unencrypted HTTP flows for analysis and threat hunting. Note that HTTP flows are not decrypted. A summary of the request and response details include the following request and response details: • HTTP method and Request URL (URI) • User-agent • content-type headers • HTTP status codes The first three HTTP events of the total number of events are displayed. A badge displays the total number of events that have been logged for the event. Click **All HTTP Events** to view all of the events on the Events Overview page. Click each event to view more details, such as header information. You cannot search or filter within the HTTP events at this time. The HTTP details are truncated to the following limitations: • The header name displays up to 64 bytes. • The header value displays up to 512 bytes. • The total header size per direction (for example, name and body) displays up to 4096 bytes. • The request and response body displays up to 512 bytes. • The request and response is Base64 encoded, by default. You can view the decoded body.
DNS	This reports the DNS query and all of the associated response details for the event. A summary of the request and response details include the following request and response details: • Request details • Query name: This is the Resource Requested (RR) name of the DNS server that the CylanceGATEWAY agent queried. • Query type: This is the type of DNS query (for example, A, AAAA, or SRV record) that was sent to the DNS server. • Response details • Resource record name: This is the name of the DNS server that is responding to the query from the CylanceGATEWAY agent. • Resource record type: This is the type of DNS response (for example, A) that was sent to the DNS server. • Resource data: This is the address of the DNS server that is returning the response. • TTL: This is the time in seconds that the requested resource data remains valid. A badge displays the total number of responses for the DNS query.

Monitoring sensitive files with CylanceAVERT

You can monitor activity and events associated with sensitive files, both at rest and in transit. All of the sensitive files in your organization display in the File Inventory. Files that have been involved in an exfiltration event display in the CylanceAVERT Events view and the Evidence Locker.

Note: If CylanceAVERT is not enabled for your tenant, the menu options to configure it are not displayed in the management console.

CylanceAVERT events

Data exfiltration events are saved and listed on the CylanceAVERT events page. CylanceAVERT events are stored in the events list for 30 days. When a data exfiltration event occurs, a new list item will be added to the events list displaying the following information:

Item	Description
Detection Time	This is the date and time that the exfiltration event occurred.
Device	This is the device name of the device where the exfiltration event was found.
User	This is the first name, last name, email, department, and title of the user who committed the exfiltration event. You can click the link to view the user details page.
Activity	This is the type of activity that CylanceAVERT tagged as a data exfiltration event. The possible values are web, email, and USB.
Location	This is the location that the sensitive data was uploaded to. The value of this is dependent on the type of upload that occurred (website root domain, email domains and recipients, location of copied USB files).
Files	This is the number of files involved in the event. You can click the link to view the file details page. Multiple files may be associated with an exfiltration event.
Policy	This is the number of CylanceAVERT user policies that were violated. Multiple policies may be associated with an exfiltration event.
Data Type	This is the number of keyword or regular expression that were met to trigger the CylanceAVERT event.

View CylanceAVERT event details

When a data exfiltration event occurs, the details of the event will be listed on the CylanceAVERT events page. You can click on the row for each event to display further details about the exfiltration event, including the number of sensitive data types involved in the event, a snippet of the event, and download the file involved. The following steps outline how you can find the events page, and the actions you can take to view more details. For encrypted or password protected files, "encrypted file" will display instead of the sensitive data types.

Before you begin:

The following data collection settings must be enabled to view file snippets and download the full file. See Configure data collection settings for more information.

- Generate File Snippets
- Enable evidence file collection

The following permissions are required to view event information:

- View general events list
- View device names
- View user names
- View policy names
- Link to policy details
- View data entities
- View file details
- Download full file

1. In the management console, on the menu bar, click **CylanceAVERT > Events**.
2. Click a row to view more details about an event.
3. In the **Event Details** pane, do any of the following:

    - Under **User details**, click the user's name to be directed to the user's information page where you can view any policies, events, or devices associated with the user.
    - Under **Policy Violations**, click on a policy to view more information about the policy that was violated.
    - Under **File details**, click the information icon to view details about the file, including what type of file it is, the sensitive data types that were scanned, and the number of occurrences of those data types. You can click 👁 to view snippet information about the exfiltration event. You can also click ⬇ to download the file involved in the exfiltration event. Evidence files are downloaded as a compressed .gz file. You will need a utility tool, such as 7zip, to decompress the files and view them.

View the file inventory to identify sensitive files

When CylanceAVERT is installed on your device, the endpoint trawling process will automatically begin to discover all the files on the device that contain the sensitive data types as specified in the information protection policies. The files that get flagged as containing sensitive organizational documents are added to the file inventory. The file inventory lets you see the number and type of sensitive documents in your environment, as well as what users and devices have access to sensitive data for risk assessment. You can also group the File Inventory list by users, devices, and data types.

Note: The trawling process may take several hours to fully complete after CylanceAVERT is installed.

Before you begin:

The following permissions are required in order to view the file inventory:

- Read file summary
- List and read policies

1. In the management console, on the menu bar, click **CylanceAVERT > File Inventory**.

    The CylanceAVERT file inventory is a list of all the files that contain sensitive data types, as specified in the information protection policies, that were discovered during the file trawling process. The supported file types are .pdf, .ooxml (Microsoft Word, Excel, and PowerPoint), .txt, .rtf, .zip, and .csv. The following table explains the information that is displayed in the file inventory list.

Item	Description
File name	This is the name of the file.
File size	This is the size of the file in KB
Info types	This is the information type that the file belongs to.
Data types	This is the number of sensitives data types that were found in the file.
Users	This is the number of users that have access to the file.
Devices	This is the number of devices that have access to the file.
Policies	This is the policy or policies that this file is a part of.
Type	This is the file type. The supported file types are .pdf, .ooxml (Microsoft Word, Excel, and PowerPoint), .txt, .rtf, .zip, and .csv.

Note: There is no pagination for this list, you can scroll to load more results or use the filter options.

Once the initial trawling process is competed, CylanceAVERT will regularly poll to check for new sensitive data. If a file is only partially scored and sensitive information was detected, an icon displays beside the file in the table and detailed views with an alert stating that the file was only partially analyzed.

2. Do any of the following:

   - To filter the file name or info types columns, click ≡ in the column heading.
   - To change which columns are displayed, click ||| on the right of the column headings.
   - To group the data by users, devices, or data types, select the grouping from the drop-down menu. From the group file inventory view, you can click on an item to display detailed information for that group.

   Note: You can view the file name and attributes in the file inventory, but file snippets and full file access are not supported.
3. You can click on an item in the file inventory to display the file details menu. From this menu, you can see the file details, the users with access to the file, the devices with access to the file, the data types found in the file, and the policies that the file violates.

View partially analyzed files

CylanceAVERT provides visibility into files that are only partially analyzed. When CylanceAVERT can not fully determine the sensitivity of a file, it appears in the Partially Analyzed Files list. The following are situations in which a file may be only partially analyzed:

- The file is large enough that the scoring engine was not able to fully complete its analysis before the file was exfiltrated.
- The file is a compressed zip file with multiple levels of hierarchy, where only the initial levels were analyzed.

Based on their sensitivity scores, there are two possible outcomes for a partially analyzed file. Either the file is partially scored and sensitive data is found, or the file is partially scored and sensitive data is not found.

If a file is partially scored and sensitive information is not detected, the file appears in the Partially Analyzed Files list with an alert stating that it was only partially analyzed.

If a file is partially scored and sensitive information is detected, it will be treated the same as a fully scored file, and it appears in the File Inventory, Events view, and Evidence Locker. However, an icon displays beside the file in the tables and detailed views with an alert stating that it was only partially analyzed.

You can view a list of files that were not fully scored by CylanceAVERT in the Partially Analyzed Files view.

1. In the management console, on the menu bar, click **CylanceAVERT > Partially Analyzed Files**.

Column	Description
File Name	The is the name of the partially analyzed file.
Time Added	This is the time that the partially analyzed file was added to the list.
File Size	This is the size of the partially analyzed file.
Extension	This is the extension type of the partially analyzed file.

Note: There is no pagination for this list. You can scroll to load more results or use the filter options.

2. Do any of the following:
   - To filter the file name or extension columns, click ≡ in the column heading.
   - To change which columns are displayed, click ||| on the right of the column headings.
3. You can click on an item in the partially analyzed files list to display the file details menu. From this menu, you can see the file details, the users with access to the file, the devices with access to the file, and the data types found in the file.

Use the evidence locker to view exfiltration event details

When a file in your file inventory is involved in a data exfiltration event, it is stored and encrypted in the BlackBerry managed AWS instance using different keys for each tenant, and it is added to the evidence locker. You can view or download the files involved in exfiltration events from the evidence locker.

Before you begin:

Evidence file collection must be enabled in the information protection settings. See Configure data collection settings for more information.

1. In the management console, on the menu bar, click **Avert > Evidence Locker**.

   The evidence locker displays a list of all the files in your organization that have been involved in a data exfiltration event. The following table explains the information that is in the Evidence Locker list:

Item	Description
Time Added	This is the time the file was added to the evidence locker.
File Name	This is the name of the file involved in an exfiltration event.
File Size	This is the size of the file involved in an exfiltration event.
Associated Events	These are the exfiltration events that the file is associated with. You can click on the number to see more details.

Item	Description
Download	You can click this to download the full file involved in the exfiltration event. Evidence files are downloaded as a compressed .gz file. You will need a utility tool, such as 7zip, to decompress the files and view them.

2. Click on the number in the associated events column to view the CylanceAVERT events.
3. To filter the time added, file name, or file size columns, click ≡ in the column heading.

View mobile OS vulnerabilities

You can use the management console to view a collective list of the Common Vulnerabilities and Exposures (CVE), as identified, defined, and tracked by the National Vulnerability Database, for any mobile OS in your organization's environment that the CylancePROTECT Mobile app is installed on. For each OS version, you can view the number of devices that use that version, the total CVE count for that OS version, the risk classification and brief description of each CVE, and a link to view full details in the National Vulnerability Database.

1. In the management console, on the menu bar, click **Protection > Vulnerabilities**.
2. Click the **Mobile OS** tab. Do any of the following:
    - To sort the vulnerabilities in ascending or descending order by a column, click the name of the column.
    - To filter the vulnerabilities, click ≡ on a column and type or select the filter criteria.
3. To view a list of vulnerabilities for an OS version, click the link in the **Total CVE** column. Click a CVE link to view details in the National Vulnerability Database.

Auditing administrator actions

You can use the audit log to view and export information about the actions performed by your organization's administrators.

View the audit log

1. In the management console, click 👤 > **Audit Log**.
2. In the filter fields, specify the criteria that you want to use to filter the audit log information.
3. To export the results to a .csv file, click ↗. Select the scope of the export and click **Export**.

   You can export a maximum of 50,000 records at once. You can see the number of results at the bottom of the screen. To export more than 50,000 records, you can filter the results (for example, by date) and export, then apply a different filter and export, and so on.

Audit log information: General administration

The following table lists the information that is added to the audit log for administrative actions that impact multiple Cylance Endpoint Security features. You can use the filtering options in the console to filter the audit log results.

Category	Action	Details
Agent Update	Edit	Rule: <*rule name*>; Zones: <*zones*>; Agent Version: <*version*>; Optic Version: <*version*>
Agent Update	Edit	Tier: <*tier name*>; Zones: N/A; Agent Version: <*version*>; Optic Version: <*version*>
Custom Update Rule	Add	Custom updater rule: <*rule name*>; Zones: <*zones*>; Agent Version: <*version*>; Optic Version: <*version*>
Custom Update Rule	Remove	Custom updater rule <*rule ID*> is deleted.
Device	Add	Device: <*device name*>; Zone: <*zone name*>
Device	Edit	Renamed: <*original name*> to <*new name*>; Policy Changed: <*old policy*> to <*new policy*>; Zones Removed: <*zone names*>; Zones Added: <*zone names*>; Agent Logging Level Changed: <*original value*> to <*new value*>; Agent Self Protection Level Changed: <*original value*> to <*new value*>
Device	Remove	Devices: <*device names*>
Login	Success	Provider: CylancePROTECT, Source IP: <*IP address*>
Login	Failure	—

Category	Action	Details
Policy	Add	Policy: *<policy name>*, Detection Settings changed from *<change details>*
Policy	Edit	Policy: *<policy name>*: *<change details>*
Policy	Remove	Policy: *<policy name>*
Syslog	Disabled	Syslog disabled.
Syslog	Settings Save	{*<configuration_settings>*}
Tenant Configuration	Update	Updated custom domain name to *<name>*.
Tenant Role	Add	Role: *<custom role name>*
Tenant Role	Edit	Role: *<custom role name>*
Tenant Role	Remove	Role: *<custom role name>*
User	Add	User: *<username>*; Role: *<role type>*
User	Edit	User: *<username>*; email: *<user email>*
User	Remove	Users: *<user names>*
Zone	Add	Zone: *<zone name>*; Policy: *<policy name>*; Value: *<"High" / "Low" / "Normal">*
Zone	Edit	Renamed: *<original name>* to *<new name>*; Current Policy: *<policy name>*; Policy Applied To All Devices In Zone: *<TRUE / FALSE>*; Values Assigned: *<"High" / "Low" / "Normal">*
Zone	Remove	Zones: *<zone names>*

Audit log information: CylancePROTECT Desktop

The following table lists the information that is added to the audit log for CylancePROTECT Desktop administrative actions. You can use the filtering options in the console to filter the audit log results.

Category	Action	Details
Application Setting	Custom Authentication Disable	Custom authentication disabled.
Application Setting	Custom Authentication Save	Custom authentication saved: {*<configuration_settings>*}

Category	Action	Details
Application Setting	Require Password to Uninstall Agent Save	Password to uninstall agent saved.
Application Setting	Require Password to Uninstall Agent Disable	Require password to uninstall agent disabled.
Application Setting	Installation Token Delete	Installation token was deleted.
Application Setting	Installation Token Regenerate	Installation token was generated.
Global List	Add	Source: CylancePROTECT; SHA256: *<file hash>*; FileName: *<name>*; Reason: *<value>*; Added to: Global Quarantine *or* Safe List; Category: *<value>*
Global List	Remove	SHA256: *<file hash>*
Script Global List	Add	Source: CylancePROTECT; SHA256: *<file hash>*; FileName: *<name>*; Reason: *<value>*; Added to: Script Control Exclusion List
Script Global List	Remove	SHA256: *<file hash>*
Threat	Safe List	SHA256: *<file hash>*; Category: *<value>*; Reason: *<value>*
Threat	Global Quarantine	Source: CylancePROTECT; SHA256: *<file hash>*; Reason: *<value>*
Threat Data Report	Generate Token	—
Threat Data Report	Delete Token	—

Audit log information: CylancePROTECT Mobile

The following table lists the information that is added to the audit log for CylancePROTECT Mobile administrative actions. You can use the filtering options in the console to filter the audit log results.

Category	Action	Details
End User	Add	User: *<email>*, Type: local
End User	Import	Success count: *<count>*, Failed count: *<count>*
End User	Remove	User: *<email>* A log entry is generated for each user that was removed.
End User	Assign policy	Policy: *<policy name>*, Users: *<email addresses>*

Category	Action	Details
End User	Send invitation	Users: *<email addresses>*, Success count: *<count>*, Failed count: *<count>*
Mobile Device	Remove	User: *<email>*, Device: *<device name>*, OS: *<OS family>*, OS version: *<version>* A log entry is generated for each device that was removed.
Mobile Device	Export	Filter: *<filter fields and values>* If “Everything” was selected, the Filter value is None. If “Current filter” was selected, the name and value of each field is listed.
Mobile Policy	Add	Source: Protect Mobile, Policy: *<policy name>*, *<setting names and values>*
Mobile Policy	Edit	Source: Protect Mobile, Policy: *<policy name>*, *<changed setting names and values>*
Mobile Policy	Remove	Source: Protect Mobile, Policy: *<policy name>* A log entry is generated for each policy that was removed.
Mobile Exclusions	Add	Source: Protect Mobile, Type: *<App / Developer / Domain / IP>*, Category: *< Approved / Restricted>*, Name: *<name>*, Platform: *<platform>*, Identifier: *<identifier>*, Issuer: *<issuer>*
Mobile Exclusions	Remove	Source: Protect Mobile, Type: *<App / Developer / Domain / IP>*, Name: *<name>* A log entry is generated for each exclusion that was removed.
Mobile Alerts	Ignore	Source: Protect Mobile, ID: *<ID>*, Type: *<alert_type>*, Name: *<alert_name>*, Description: *<device_OS>* A log entry is generated for each alert that was ignored.
Mobile Alerts	Export	Source: Protect Mobile, Filter: *<filter fields and values>* If “Everything” was selected, the Filter value is None. If “Current filter” was selected, the name and value of each field is listed.

Audit log information: CylanceOPTICS

The following table lists the information that is added to the audit log for CylanceOPTICS administrative actions. You can use the filtering options available in the console to filter the audit log results.

Category	Action	Details
Advanced Query	Execute	Query: *<EQL_query>*

Category	Action	Details
Advanced Query Export	Add	Name: *<name>*; Description: *<description>*; Shared: *<isShared>*
Advanced Query Export	Download	Name: *<name>*; Description: *<description>*
Advanced Query Export	Remove	Name: *<name>*; Description: *<description>*; Shared: *<isShared>*
Advanced Query Snapshot	Add	Name: *<name>*; Description: *<description>*; Shared: *<isShared>*
Advanced Query Snapshot	Edit	Name: *<name>*; Description: *<description>*; Shared: *<isShared>*
Advanced Query Snapshot	Remove	Name: *<name>*; Description: *<description>*; Shared: *<isShared>*
Advanced Query Template	Add	Name: *<name>*; Description: *<description>*; Shared: *<isShared>*; Query: *<EQL_query>*
Advanced Query Template	Edit	Name: *<name>*; Description: *<description>*; Shared: *<isShared>*; Query: *<EQL_query>*
Advanced Query Template	Remove	Name: *<name>*; Description: *<description>*; Shared: *<isShared>*
Detections	Change Status	Detection: *<detection label>*; Detection ID: *<detection id>*; Device: *<device name>*; Previous Status: *<previous detection status>*; New Status: *<new detection status>*
Detections	Remove	Detection: *<detection label>*; Detection ID: *<detection id>*; Device: *<device name>*
Detection Exception	Add	Name: *<name>*
Detection Exception	Edit	Name: *<name>*
Detection Exception	Remove	Name: *<name>*
Detection Rule	Add	Name: *<name>*; Description: *<description>*; Severity: *<severity>*; OS: *<OS list>*
Detection Rule	Edit	Name: *<name>*; Description: *<description>*; Severity: *<severity>*; OS: *<OS list>*

Category	Action	Details
Detection Rule	Remove	Name: *<name>*; Description: *<description>*; Severity: *<severity>*; OS: *<OS list>*
Detection Rule Set	Add	Name: *<name>*; Description: *<description>*; Device Policy: *<device policy name>*
Detection Rule Set	Edit	Name: *<name>*; Description: *<description>*; Device Policy: *<device policy name>*
Detection Rule Set	Remove	Name: *<name>*; Description: *<description>*; Device Policy: *<device policy name>*
Device	File Download	Device: *<device name>*; File: *<file path and name>*
Device	Lock	Device: *<device name>*; Configuration Profile: *<profile name>*; Lockdown Period: *<lockdown period>*
Device	Unlock	Device: *<device name>*
Device	Change Lockdown Profile	Device: *<device name>*; Configuration Profile: *<profile name>*
Device	Show Unlock Key	Device: *<device name>*
Focus Data	Add	Device: *<device name>*; Type: *<focus view type>*; Artifact: *<focus view artifact>*
InstaQuery	Add	Name: *<IQ name>*, Artifact: *<IQ artifact>*, Facet: *<IQ facet>*, Term: *<IQ term>*
InstaQuery	Remove	Name: *<IQ name>*, Artifact: *<IQ artifact>*, Facet: *<IQ facet>*, Term: *<IQ term>*
Job Service	Stop	Name: *<name>*; Service: *<parent service type>*
Lockdown Configuration	Add	Configuration Profile: *<configuration profile>*; Description: *<description>*; Whitelist Definitions: *<allowed_connections>*
Lockdown Configuration	Delete	Configuration Profile: *<configuration profile>*
Lockdown Configuration	Edit	Configuration Profile: *<configuration profile>*; Description: *<description>*; Whitelist Definitions: *<allowed_connections>*
Package Deploy	Add	Name: *<name>*; Packages: *<packages>*
Package Deploy	Remove	Name: *<name>*
Package PlayBook	Add	Name: *<name>*; Packages: *<packages>*

Category	Action	Details
Package PlayBook	Edit	Name: *<name>*; Packages: *<packages>*
Package PlayBook	Remove	Name: *<name>*; Packages: *<packages>*
PlayBook Result	Remove	Device: *<device name>*; Playbook Name: *<playbook name>*; Detection ID: *<detection id>*; Status: *<status>*
Remote Response	Connect	Device: *<device name>*
Remote Response	Disconnect	Device: *<device name>*
Scheduled Advanced Query	Add	Name: *<name>*; Description: *<description>*; Shared: *<isShared>*; Schedule: *<schedule_details>*
Scheduled Advanced Query	Edit	Name: *<name>*; Description: *<description>*; Shared: *<isShared>*; Schedule: *<schedule_details>*
Scheduled Advanced Query	Remove	Name: *<name>*; Description: *<description>*; Shared: *<isShared>*
Scheduled Advanced Query	Remove Result	Name: *<name>*; Description: *<description>*; Result Timestamp: *<result_timestamp>*; Results: *<result_count>*
Scheduled Advanced Query	Start	Name: *<name>*; Description: *<description>*; Shared: *<isShared>*; Schedule: *<schedule_details>*
Scheduled Advanced Query	Stop	Name: *<name>*; Description: *<description>*; Shared: *<isShared>*; Schedule: *<schedule_details>*

Audit log information: CylanceAVERT

The following table lists the information that is added to the audit log for CylanceAVERTadministrative actions. You can use the filtering options in the console to filter the audit log results.

<table>
<tr><th>Category</th><th>Action</th><th>Details</th></tr>
<tr><td>Data Entity</td><td>Add</td><td>

```
{
    "id": "<ID>",
    "tenantId": "<Tenant ID>",
    "occurred": "<Date/Time>",
    "traceId": "<Trace ID>",
    "spanId": "<Span ID>",
    "source": "com.blackberry.dlp",
    "type": "AUDIT",
    "category": "Entity",
    "subcategory": "created",
    "message": "admin created DataEntity
 named <Policy name>"
    },
    "admin": {
        "ecoId": "<Eco ID>"
    },
    "entity": {
        "id": "<ID>",
        "type": "DATAENTITY",
        "displayName": "<Entity display name>"
    },
    "changes": {
        "regions": {
            "new": "<Region>"
        },
        "name":{
            "new": "<Data entity name>"
        "description": {
            "new": "<Description>"
        },
        "infoTypes": {
            "new": "<Info types>"
        },
        "Type": {
            "new": "<Data type>"
        },
        "Parameters": {
            "new": "<parameters>"
        },
        "algorithm":{
            "new":<Algorithm>
     }
}
```

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

<table>
<tr><th>Category</th><th>Action</th><th>Details</th></tr>
<tr><td>Data Entity</td><td>Edit</td><td>

```
{
    "id": "<ID>",
    "tenantId": "<Tenant ID>",
    "occurred": "<Date/Time>",
    "traceId": "<Trace ID>",
    "spanId": "<Span ID>",
    "source": "com.blackberry.dlp",
    "type": "AUDIT",
    "category": "ENTITY",
    "subcategory": "UPDATED",
    "message": "admin updated DataEntity
 named <Data entity name>",
    "crud": {
        "admin": {
            "ecoId": "<Eco ID>"
        },
        "entity": {
            "id": "<ID>",
            "type": "DATAENTITY",
            "displayName": "<Data entity
 display name>"
        },
        "changes": {
            "description": {
                "new": "<New description>",
                "old": "<Old description>"
            }
        }
    }
}
```

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

<table>
<thead>
<tr><th>Category</th><th>Action</th><th>Details</th></tr>
</thead>
<tbody>
<tr><td>Data Entity</td><td>Remove</td><td><pre>
{
    "id": "<ID>",
    "tenantId": "<Tenant ID>",
    "occurred": "<Date/Time>",
    "traceId": "<Trace ID>",
    "spanId": "<Span ID>",
    "source": "com.blackberry.dlp",
    "type": "AUDIT",
    "category": "ENTITY",
    "subcategory": "DELETED",
    "message": "admin deleted DataEntity
 named <Data entity name>",
    "crud": {
        "admin": {
            "ecoId": "<Eco ID>"
        },
        "entity": {
            "id": "<ID>",
            "type": "DATAENTITY",
            "displayName": "<Data entity
 display name>"
        }
    }
}
</pre></td></tr>
<tr><td>Evidence File</td><td>Download</td><td><pre>
{
    "id": "<ID>",
    "tenantId": "<Tenant ID>",
    "occurred": "<Date/Time>",
    "traceId": "<Trace ID>",
    "spanId": "<Span ID>",
    "source": "com.blackberry.dlp",
    "type": "AUDIT",
    "category": "ENTITY",
    "subcategory": "READ",
    "message": "Evidence File is downloaded",
    "crud": {
        "admin": {
            "ecoId": "<Eco ID>"
        },
        "entity": {
            "id": "<ID>",
            "type": "<Entity type>"
        }
    }
}
</pre></td></tr>
</tbody>
</table>

<table>
<tr><th>Category</th><th>Action</th><th>Details</th></tr>
<tr><td>Evidence File</td><td>Remove</td><td>

```
{
    "id": "<ID>",
    "tenantId": "<Tenant ID>",
    "occurred": "<Date/Time>",
    "traceId": "<Trace ID>",
    "spanId": "<Span ID>",
    "source": "com.blackberry.dlp",
    "type": "AUDIT",
    "category": "ENTITY",
    "subcategory": "DELETED",
    "message": "Evidence File is DELETED",
    "crud": {
        "admin": {
            "ecoId": "<Eco ID>"
        },
        "entity": {
            "id": "<ID>",
            "type": "<Entity type>"
        }
    }
}
```

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

Category	Action	Details
Policy	Add	

```
{
    "common": {
        "id": "<ID>",
        "tenantId": "<Tenant ID>",
        "occurred": "<Date/Time>",
        "traceId": "<Trace ID>",
        "spanId": "<Span ID>",
        "source": "com.blackberry.dlp",
        "type": "AUDIT",
        "category": "Entity",
        "subcategory": "created",
        "message": "admin created Policy
 named <Policy name>"
    },
    "admin": {
        "ecoId": "<Eco ID>"
    },
    "entity": {
        "id": "<ID>",
        "type": "PROFILE",
        "displayName": "<Entity display name>"
    },
    "changes": {
        "emailDomainsRule": {
            "new": "<Domain rule>"
        },
        "condition": {
            "new": "<Condition>"
        },
        "policyName": {
            "new": "<Policy name>"
        },
        "policyType": {
            "new": "<Policy type>"
        },
        "description": {
            "new": "<Description>"
        },
        "policyRules": {
            "new": "<Policy rules>"
        },
        "classification": {
            "new": "<Classification>"
        },
        "browserDomains": {
            "new": "<Browser domains>"
        }
    }
}
```

Category	Action	Details
Policy	Edit	

```
{
    "common": {
        "id": "<ID>",
        "tenantId": "<Tenant ID>",
        "occurred": "<Date/Time>",
        "traceId": "<Trace ID>",
        "spanId": "<Span ID>",
        "source": "com.blackberry.dlp",
        "type": "AUDIT",
        "category": "Entity",
        "subcategory": "Updated",
        "message": "admin created Policy
 named <Policy name>"
    },
    "admin": {
        "ecoId": " "
    },
    "entity": {
        "id": "fbfa8366-
e58c-4018-925f-2a536dce4c2d",
        "type": "PROFILE",
        "displayName": "policy-test-name-
created-from-auto-test"
    },
    "changes":
{
    "policyName":{
              "old" : "HIPAA",
              "new" : "HIPAA Compliance"
        },

    "condition": {
          "old": "<Old condition>",
          "new":"<New condition>"
      },

    "policyRules": {
            "old":[{<Old policy rules>}],
            "new":[{<New policy rules>}]
      },

    "policyConfigs": {
            "old":[{<Old policy rules>}],
            "new":[{<New policy rules>}]
      },

    "browserDomains":{
            "old":<Old browser domains>,
            "new":<New browser domains>
      },

    "emailDomainsRule": {
            "old":<Old domain rule>,
            "new":<New domain rule>
      }
    }
}
```

<table>
<tr><th>Category</th><th>Action</th><th>Details</th></tr>
<tr><td>Policy</td><td>Remove</td><td><pre>
{
    "id": "<ID>",
    "tenantId": "<Tenant ID>",
    "occurred": "<Date/Time>",
    "traceId": "<Trace ID>",
    "spanId": "<Span ID>",
    "source": "com.blackberry.dlp",
    "type": "AUDIT",
    "category": "ENTITY",
    "subcategory": "DELETED",
    "message": "admin DELETED Policy
 named <Policy name>",
    "crud": {
        "admin": {
            "ecoId": "<Eco ID>"
        },
        "entity": {
            "id": "<ID>",
            "type": "PROFILE",
            "displayName": "<Entity display
 name>"
        }
    }
}
</pre></td></tr>
<tr><td>Setting</td><td>Update</td><td><pre>
{
    "id": "<ID>",
    "tenantId": "<Tenant ID>",
    "occurred": "<Date/Time>",
    "traceId": "<Trace ID>",
    "spanId": "<Span ID>",
    "source": "com.blackberry.dlp",
    "type": "AUDIT",
    "category": "SETTING",
    "subcategory": "UPDATED",
    "message": "admin UPDATED DLP settings",
    "crud": {
        "admin": {
            "ecoId": "<Eco ID>"
        },
        "changes": {

 "ui.tenant.setting.emailRecipients": {
                "new": "<New email
 recipients>",
                "old": "<Old email
 recipients>"
            }
        }
    }
}
</pre></td></tr>
</table>

<table>
<thead>
<tr><th>Category</th><th>Action</th><th>Details</th></tr>
</thead>
<tbody>
<tr><td>Template</td><td>Remove</td><td><pre>
{
    "id": "<ID>",
    "tenantId": "<Tenant ID>",
    "occurred": "<Date/Time>",
    "traceId": "<Trace ID>",
    "spanId": "<Span ID>",
    "source": "com.blackberry.dlp",
    "type": "AUDIT",
    "category": "ENTITY",
    "subcategory": "DELETED",
    "message": "Template <Template name> was
 deleted",
    "crud": {
        "admin": {
            "ecoId": "<Eco ID>"
        },
        "entity": {
            "id": "<ID>",
            "type": "TEMPLATE",
            "displayName": "<Template name>"
        }
    }
}
</pre></td></tr>
</tbody>
</table>

<table>
<tr><th>Category</th><th>Action</th><th>Details</th></tr>
<tr><td>Template</td><td>Add</td><td>

```
{
    "id": "<ID>",
    "tenantId": "<Tenant ID>",
    "occurred": "<Date/Time>",
    "traceId": "<Trace ID>",
    "spanId": "<Span ID>",
    "source": "com.blackberry.dlp",
    "type": "AUDIT",
    "category": "ENTITY",
    "subcategory": "CREATED",
    "message": "Template <Template name> was
 created",
    "crud": {
        "admin": {
            "ecoId": "<Eco ID>"
        },
        "entity": {
            "id": "<ID>",
            "type": "TEMPLATE",
            "displayName": "<Template name>"
        },
        "changes": {
            "condition": {
                "new": "<Condition>"
            },
            "regions": {
                "new": "<Region>"
            },
            "name": {
                "new": "<Template name>"
            },
            "description": {
                "new": <Description>"
            },
            "infoTypes": {
                "new": "Info type>"
            },
            "type": {
                "new": "<Template type>"
            }
        }
    }
}
```

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

Managing logs

This section provides information about changing log settings for different Cylance Endpoint Security features and services.

Configure BlackBerry Connectivity Node logging

The BlackBerry Connectivity Node allows you to synchronize with an on-premises Microsoft Active Directory or LDAP directory to add users and user groups who are enabled for the CylancePROTECT Mobile app and for CylanceGATEWAY.

You can set the logging level, syslog information, and local file information for BlackBerry Connectivity Node events.

1. In the management console, on the menu bar, click **Settings > Directory Connections**.
2. On the **Connectivity Node** tab, click **Settings**.
3. From the **Server debug levels** drop-down menu, select the level of event you want to log.
4. To send logs to SysLog, click the button beside **SysLog** and fill in the **Host** and **Port** fields.
5. To send logs to the computer that the BlackBerry Connectivity Node is installed on, click the button beside **Enable local file destination**.
6. Fill in the fields for **Maximum log file size** in MB and **Maximum server log file age** (in days).
7. To compress the logs folder, click the button beside **Enable logging folder compression**.
8. Click **Save**.

Manage logs for the CylancePROTECT Desktop agent

The log files of the CylancePROTECT Desktop agent provide useful information for troubleshooting issues. When troubleshooting, enable verbose logging and reproduce the issue to capture relevant information in the log file. Verbose logging creates a larger log file, so it should be used for troubleshooting purposes only. Agent log files are retained for 30 days in the management console.

1. In the management console, on the menu bar, click **Assets > Devices**.
2. Click a device.
3. Do any of the following:
   - If you want to change the log level, in the **Agent Logging Level** drop-down list, click the log level.

     If you change the log level to verbose, see Enable verbose logging on a CylancePROTECT Desktop device.
   - To obtain the CylancePROTECT Desktop agent log file, under **Threats & Activities**, on the **Agent Logs** tab, click **Upload Current Log File**. This option is available only if the device is online.

Enable verbose logging on a CylancePROTECT Desktop device

Before you begin: In the management console, set the CylancePROTECT Desktop agent log level to verbose.

Follow the steps for the device OS:

OS	Steps

Windows	**a.** Right-click the agent icon in the system tray and click **Exit**.
	b. Open the command line as an administrator.
	c. Run the following command:
	`cd C:\Program Files\Cylance\Desktop`
	d. Run the following command:
	`CylanceUI.exe -a`
	e. Right-click the agent icon in the system tray and click **Logging > All**.

macOS	**a.** Exit the currently running user interface. **b.** Execute the following command from terminal: `sudo /Applications/Cylance/CylancePROTECTUI.app/ Contents/MacOS/CylancePROTECTUI.-a` **c.** Right-click the agent icon in the system tray and select **Logging > All**.

Linux logging

Review the following sections for information about setting the logging level and collecting the agent log files.

Set the logging level

The logging level that is set determines the level of detail in the agent logs. Note that with verbose logging, the size of the log file increases very quickly.

Before you begin: You can use the following command to view the current logging level for the Linux agent:

```
/opt/cylance/desktop/cylance -l
```

To set the logging level, use the following command:

```
/opt/cylance/desktop/cylance -L <level>
```

The value of *<level>* can be one of the following:

- `0`: Error
- `1`: Warning
- `2`: Information
- `3`: Verbose

For example, the following command sets the logging level to "Verbose".

```
/opt/cylance/desktop/cylance -L 3
```

Collect agent log files from Linux devices

Use the following commands to gather agent log files from a Linux device. Log files are stored on the device for 30 days. You must have root permissions to gather log files.

Red Hat and CentOS:

```
ps aux > ~/ps.txtph product="Cylance">sudo pmap -x $(ps -e | grep cylancesvc | cut
 -d ‘ ‘ -f 1) > ~/maps.txt
cat /proc/cpuinfo > ~/cpu.txt
cat /proc/meminfo > ~/mem.txt
cat /proc/mounts > ~/mounts.txt
cat /proc/modules > ~/modules.txt
cat /proc/slabinfo > ~/slabinfo.txt
tar -cvzf cylancelogs-$(date --rfc-3339=’date’).tgz /var/log/messages* /opt/
cylance/desktop/log ~/maps.txt ~/cpu.txt ~/mounts.txt ~/modules.txt ~/ps.txt ~/
mem.txt ~/slabinfo.txt
```

Ubuntu:

```
ps aux > ~/ps.txt
sudo pmap -x $(ps -e | grep cylancesvc | cut -d ‘ ‘ -f 2) > ~/maps.txt
cat /proc/cpuinfo > ~/cpu.txt
cat /proc/meminfo > ~/mem.txt
cat /proc/mounts > ~/mounts.txt
cat /proc/modules > ~/modules.txt
cat /proc/slabinfo > ~/slabinfo.txt
tar -cvzf cylancelogs-$(date --rfc-3339=’date’).tgz /var/log/syslog* /opt/
cylance/desktop/log ~/ps.txt ~/maps.txt ~/cpu.txt ~/mounts.txt ~/modules.txt   ~/
slabinfo.txt  ~/mem.txt
```

Amazon and SUSE Linux:

```
ps aux > ~/ps.txt
sudo pmap -x $(ps -e | grep cylancesvc | cut -d ' ' -f 2) > ~/maps.txt
cat /proc/cpuinfo > ~/cpu.txt
cat /proc/meminfo > ~/mem.txt
cat /proc/mounts > ~/mounts.txt
cat /proc/modules > ~/modules.txt
cat /proc/slabinfo > ~/slabinfo.txt
tar -cvzf cylancelogs-$(date --rfc-3339='date').tgz /var/log/messages* /opt/
cylance/desktop/log ~/ps.txt ~/maps.txt ~/cpu.txt ~/mounts.txt ~/modules.txt ~/
slabinfo.txt
```

Send events to a SIEM solution or syslog server

Security Information and Event Management (SIEM) software collects, analyzes, and aggregates security data from multiple sources to detect potential security threats. You can choose to send the events detected by Cylance Endpoint Security solutions to your organization’s SIEM software or syslog server. The alert data that is sent to a SIEM or syslog server is the same alert data that is displayed in the management console. For more information about the specific events reported by Cylance Endpoint Security solutions, see the Syslog Guide.

1. In the management console, on the menu bar, click **Settings > Application**.
2. Select the **Syslog/SIEM** check box.
3. Select the events that you want to send to your organization's SIEM or syslog integration. For more information about each event type, see the Syslog Guide.
4. Specify the information for your SIEM or syslog integration. For more information, see the Syslog Guide.
5. Click **Test Connection** to verify the settings.
6. Click **Save**.

Enable access to the Cylance User API

Cylance Endpoint Security supports integration with third-party programs using the Cylance User API, a set of RESTful APIs. This allows your organization to programmatically manage Cylance Endpoint Security settings and configurations. Administrators can customize integration settings to control which API privileges a user has. For security, an API user needs an application ID and an application secret that you generate when you add a custom application in the management console. A tenant can have up to 10 custom integrations.

For more information, see the Cylance User API guide.

Note: In July 2022, a security enhancement was introduced for existing Cylance Endpoint Security tenants. Users with the Administrator role can enable a new feature that permanently removes application secrets from the management console after they are generated, ensuring that they cannot be viewed by any users with access to the Cylance console. If you enable this feature in Settings > Integrations, when an administrator generates or regenerates an application secret, it will display only until the administrator dismisses the dialogue or navigates away from the screen. The app secret will not display in the list. To remove your existing application secrets and enable this behavior, you can expand **Improved Security Available** and click **Remove Secret**. After you enable the feature, any application secrets that were generated previously will no longer be available to view. You should record existing application secrets before you enable this feature. You cannot revert to the previous behavior that exposes application secrets in the console. You can generate new application IDs and secrets as necessary.

For new Cylance Endpoint Security tenants created after July 2022, this feature is enabled by default.

1. In the management console, click **Settings > Integrations**.
2. Click **Add Application**.
3. Enter a name for the application.
4. Select the API privileges to allow access to.
5. Click **Save**.

   The application ID and application secret display.
6. Click **OK**.

Troubleshooting Cylance Endpoint Security

This section provides guidance for troubleshooting Cylance Endpoint Security services and features.

Using the BlackBerry Support Collection Tool

If you are working with BlackBerry Support to resolve an issue, you can download the BlackBerry Support Collection Tool to gather product data and system information. For more information, visit support.blackberry.com to read article 66596.

Using the Report a problem feature

The CylanceGATEWAY agent and CylancePROTECT Mobile app include a Report a problem option that users can use to send a problem report and agent log files to BlackBerry without contacting their IT administrator for troubleshooting assistance. BlackBerry recommends that you instruct users to contact their IT administrator for troubleshooting assistance before they submit the report and agent log files to BlackBerry. For more information, see the CylanceGATEWAY agent settings and Report a problem to BlackBerry,

Removing the BlackBerry Connectivity Node software from Cylance Endpoint Security

You can use the uninstall application to remove the BlackBerry Connectivity Node software from the server that it is installed on. Uninstalling the BlackBerry Connectivity Node does not remove it from the Cylance Endpoint Security management console. Therefore, if you want to reinstall the BlackBerry Connectivity Node software at a later date, you must first remove the BlackBerry Connectivity Node instance from the management console.

To remove the BlackBerry Connectivity Node software, perform the following actions:

Step	Action
1	Remove the BlackBerry Connectivity Node software from the local server.
2	Remove all Active Directory users that are associated with all directory connections that you want to remove.
3	Remove user groups associated with all directory connections that you want to remove.
4	Remove the BlackBerry Connectivity Node instance from the Cylance Endpoint Security management console.

Remove the BlackBerry Connectivity Node software from the local server

If you are troubleshooting, back up `\Program Files\BlackBerry\BlackBerry Connectivity Node - UES\Logs` before you uninstall the software.

1. On the taskbar, click **Start > Control Panel > Programs > Programs and Features**.
2. Click **BlackBerry Connectivity Node - UES**.
3. Click **Uninstall**.
4. Click **Next**.
5. Click **Close**.
6. Restart the computer to finish removing the BlackBerry Connectivity Node software.

Remove a BlackBerry Connectivity Node instance from the Cylance Endpoint Security management console

If you uninstall a BlackBerry Connectivity Node instance, you must complete the following steps to remove the data for that instance from the Cylance Endpoint Security database. If you do not, the BlackBerry Connectivity Node entry in the Cylance Endpoint Security management console will remain and its state is displayed as "Paused."

Before you begin:

- Remove the BlackBerry Connectivity Node software from the local server.
- Make sure that you are signed in as a user that has permission to remove the instance. By default, this is the Security Administrator or Enterprise Administrator role.

1. In the management console, on the menu bar, click **Settings > Directory connections > Connectivity Node**.
2. Click the **Connectivity Node** tab.
3. Click 🗑 beside the BlackBerry Connectivity Node that you want to remove.
4. Click **Delete**.

Troubleshooting CylancePROTECT Desktop

This section provides information to help you troubleshoot and resolve issues with CylancePROTECT Desktop.

Remove the CylancePROTECT Desktop agent from a device

Before you begin:

- For the devices that you want to remove the CylancePROTECT Desktop agent from, assign a device policy with no settings enabled. Verify that **Protection Settings > Prevent service shutdown from device** and **Application Control** are turned off in the policy.
- If you require users to provide a password to remove the CylancePROTECT Desktop agent, note the password.

1. Use one of the following methods to remove the agent from a device:

   Windows

   - To manually remove CylancePROTECT Desktop, use Add/Remove programs. If an uninstall password is required, you must use the command line method below with the password protection command.
   - Run the command prompt as an administrator and use one of the following commands:
     - CylancePROTECTSetup.exe:

       ```
       CylancePROTECTSetup.exe /uninstall
       ```
     - CylancePROTECT_x64.msi standard:

       ```
       msiexec /uninstall CylancePROTECT_x64.msi
       ```

    - CylancePROTECT_x64.msi Windows installer:

      ```
      msiexec /x CylancePROTECT_x64.msi
      ```
    - CylancePROTECT_x86.msi standard:

      ```
      msiexec /uninstall CylancePROTECT_x86.msi
      ```
    - CylancePROTECT_x86.msi Windows installer:

      ```
      msiexec /x CylancePROTECT_x86.msi
      ```
    - Product ID GUID standard:

      ```
      msiexec /uninstall {2E64FC5C-9286-4A31-916B-0D8AE4B22954}
      ```
    - Product ID GUID Windows installer:

      ```
      msiexec /x {2E64FC5C-9286-4A31-916B-0D8AE4B22954}
      ```

Optional commands:

- Quiet uninstall:

  ```
  /quiet
  ```
- Quiet and hidden:

  ```
  /qn
  ```
- Password protection:

  ```
  UNINSTALLKEY="<password>"
  ```
- Auto quarantined files:

  ```
  QUARANTINEDISPOSETYPE=<0_or_1>
  ```

    - 0 deletes all files
    - 1 restores all files
- Generate uninstall log file:

  ```
  /Lxv* <path_including_file_name>
  ```

macOS

Run the following command:

```
sudo /Applications/Cylance/Uninstall\ CylancePROTECT.app/Contents/MacOS/
Uninstall\ CylancePROTECT
```

If an uninstall password is required, add the following parameter:

```
--password=<password>
```

Linux

a. Use one of the following commands to uninstall the agent:

- RHEL/CentOS:

  ```
  rpm -e $(rpm -qa | grep -i cylance)
  ```

- Ubuntu/Debian:

  ```
  dpkg -P cylance-protect cylance-protect-ui cylance-protect-driver cylance-
  protect-open-driver
  ```

- Amazon Linux 2/SUSE:

  ```
  rpm -e $(rpm -qa | grep -i cylance)
  ```

b. Use one of the following commands to uninstall the Linux agent drivers:

- RHEL/CentOS:

  ```
  rpm -e CylancePROTECTDriver CylancePROTECTOpenDriver
  ```

- Ubuntu/Debian:

  ```
  dpkg -P cylance-protect-driver cylance-protect-open-driver
  ```

- Amazon Linux 2:

  ```
  rpm -e CylancePROTECTDriver-<package_version>.amzn2.x86_64
  rpm -e CylancePROTECTOpenDriver-<package_version>.amzn2.86_64
  ```

2. In the management console, in **Assets > Devices**, select the device and click **Remove**. Click **Yes** to confirm.

Re-register a Linux agent

If an agent becomes unregistered from the console for any reason, the user needs to re-register the device using a token. Use one of the following commands to register the device again, replacing `token` with the installation token from the tenant:

Red Hat, CentOS, and Ubuntu:

```
/opt/cylance/desktop/cylance --register=token
```

For CentOS, you can also use the following command:

```
/opt/cylance/desktop/cylance --r=token
```

Amazon and SUSE Linux:

```
/opt/cylance/desktop/cylance -r token
```

Troubleshoot update, status, and connectivity issues with CylancePROTECT Desktop

Consider the following items when troubleshooting update, status, and connectivity issues with CylancePROTECT Desktop:

- Review the Status icons of the CylancePROTECT Desktop agent.
- Verify that firewall port 443 is open and that the device can resolve and connect to BlackBerry sites.
- Review the device information in the management console. Verify whether the device is online or offline and its last connected time.

- Verify whether a proxy is being used by the device to connect to the Internet, and whether credentials are properly configured on the proxy.
- Restart the Cylance service so that it attempts to connect to the console.
- Collect debug logs. See Manage logs for the CylancePROTECT Desktop agent.
- Collect the output of system information when the issue occurs.
    - Windows: msinfo32 or winmsd
    - macOS: System Information

A large number of DYLD Injection violations are reported by Linux devices

Possible cause

Certain third-party applications, such as Splunk, Dynatrace, AppDynamics, and DataDog, try to preload modules (LD_PRELOAD environment variable for a process), causing DYLD Injection violation events for any process monitored by the application.

Possible solution

Do the following:

1. If you are using a version of the CylancePROTECT Desktop agent earlier than 2.1.1574, upgrade to 2.1.1574 or later. BlackBerry strongly recommends upgrading to the latest available version of the agent to benefit from the latest enhancements.
2. Add memory protection exclusions for the .so components that a third-party application tries to inject. Inspect the LD_PRELOAD variable to determine the .so components that you need to add exclusions for ("man ld.so" can provide some guidance). It is a best practice to contact the support resources for the third-party application to identify the applicable .so files.

Time zone variances for CylancePROTECT Desktop

Depending on where you view date and time information for CylancePROTECT Desktop, the time zone used can vary.

Date and time displayed in this UI	Time zone used
CylancePROTECT Desktop agent (including event notifications and agent logs)	Time zone of the local machine.
Management console (except for the reports tab and exported data)	Time zone of the administrator using the console.
Reports tab in the management console	Time zone of the administrator using the console. When you export a report, the UTC time zone is used in the export.
Syslog events	UTC time zone.
Threat data report and data exported from the management console	UTC time zone.

Folder exclusions when using CylancePROTECT Desktop with third-party security products

If you use third-party security products with CylancePROTECT Desktop, you will need to configure them to exclude Cylance directories to ensure that CylancePROTECT Desktop can run simultaneously with them without issues.

CylancePROTECT directories, files, or processes to exclude in Windows

Windows version	Path

Windows (all versions)	`C:\Program Files\Cylance`
	`C:\ProgramData\Cylance`
	`C:\Documents and Settings\All Users\Application Data \Cylance\Desktop\q`
	`C:\Windows\System32\Drivers\CyProtectDrv*.sys`
	`C:\Windows\System32\Drivers\CyDevFlt*.sys`
	`C:\Windows\System32\Drivers\CylanceDrv*.sys`
	`C:\Windows\CyProtect.cache`
	`C:\Windows\CylanceUD.cache`
	`C:\Windows\Temp\CylanceDesktopArchive`
	`C:\Windows\Temp\CylanceDesktopRemoteFile`
	`C:\Program Files\Cylance\Desktop\CylanceSvc.exe`
	`C:\Program Files\Cylance\Desktop\CylanceUI.exe`
	`C:\Program Files\Cylance\Desktop\CyUpdate.exe`
	`C:\Program Files\Cylance\Desktop\LocalePkg.exe`

CylancePROTECT directories to exclude in macOS

macOS Version	Path

macOS X (10.9-10.11), macOS 10.12 and later	`/Library/Application Support/Cylance/Desktop/q`
	`/Library/Application Support/Cylance/`
	`/System/Library/Extensions/CyProtectDrvOSX.kext/`
	`/private/tmp/CylanceDesktopArchive`
	`/private/tmp/CylanceDesktopRemoteFile`

CylancePROTECT directories to exclude in Linux

The paths that are related to proxy configuration are optional exclusions. They are only required if you have a proxy override configured for CylancePROTECT.

Linux Version	Path

Amazon Linux	CylancePROTECT:
	`/opt/cylance`
	`/usr/src/CyProtectDrv-1.2`
	`/tmp/CylanceDesktopArchive`
	`/tmp/CylanceDesktopRemoteFile`
	`/lib/modules/*/extra/CyProtectDrv.ko`
	`/etc/sysconfig/modules/cylance.modules`
	`/etc/modprobe.d/cylance.conf`
	`/etc/init/cylancesvc.conf`
	`/etc/dbus-1/system.d/com.cylance.agent_server.conf`
	`/var/run/cylancesvc.pid`
	Proxy configuration (only if required):
	`/etc/init/cylancesvc.override`
	CylanceUI:
	Not available on Amazon Linux.

Amazon Linux 2
Amazon Linux 2023
	CylancePROTECT:
	`/opt/cylance`
	`/usr/src/CyProtectDrv-1.2`
	`/tmp/CylanceDesktopArchive`
	`/tmp/CylanceDesktopRemoteFile`
	`/lib/modules/*/extra/CyProtectDrv.ko`
	`/etc/sysconfig/modules/cylance.modules`
	`/etc/modprobe.d/cylance.conf`
	`/usr/lib/systemd/system/cylancesvc.service`
	`/etc/dbus-1/system.d/com.cylance.agent_server.conf`
	`/var/run/cylancesvc.pid`
	Proxy configuration (only if required):
	`/etc/systemd/system/cylancesvc.service.d/proxy.conf`
	CylanceUI:
	Not available on Amazon Linux 2 or Amazon 2023.

Linux Version	Path

RHEL/CentOS 6.x	CylancePROTECT:
	`/opt/cylance`
	`/usr/src/CyProtectDrv-1.2`
	`/tmp/CylanceDesktopArchive`
	`/tmp/CylanceDesktopRemoteFile`
	`/lib/modules/*/extra/CyProtectDrv.ko`
	`/etc/sysconfig/modules/cylance.modules`
	`/etc/modprobe.d/cylance.conf`
	`/etc/init/cylancesvc.conf`
	`/etc/dbus-1/system.d/com.cylance.agent_server.conf`
	`/var/run/cylancesvc.pid`
	Proxy configuration (only if required):
	`/etc/init/cylancesvc.override`
	CylanceUI:
	`/etc/xdg/autostart/cylance-protect.desktop`
	`/usr/share/applications/cylance-protect.desktop`

RHEL/CentOS 7.x, 8.x
Oracle Linux7, 8, 9
	CylancePROTECT:
	`/opt/cylance`
	`/usr/src/CyProtectDrv-1.2`
	`/tmp/CylanceDesktopArchive`
	`/tmp/CylanceDesktopRemoteFile`
	`/lib/modules/*/extra/CyProtectDrv.ko`
	`/etc/sysconfig/modules/cylance.modules`
	`/etc/modprobe.d/cylance.conf`
	`/usr/lib/systemd/system/cylancesvc.service`
	`/etc/dbus-1/system.d/com.cylance.agent_server.conf`
	`/var/run/cylancesvc.pid`
	Proxy configuration (only if required):
	`/etc/systemd/system/cylancesvc.service.d/proxy.conf`
	CylanceUI:
	`/etc/xdg/autostart/cylance-protect.desktop`
	`/usr/share/applications/cylance-protect.desktop`
	`/usr/share/gnome-shell/extensions/cylance-protect@cylance.com`

Linux Version	Path

SUSE (SLES) 11.x	CylancePROTECT:
	`/opt/cylance`
	`/usr/src/CyProtectDrv-1.2`
	`/tmp/CylanceDesktopArchive`
	`/tmp/CylanceDesktopRemoteFile`
	`/lib/modules/*/extra/CyProtectDrv.ko`
	`/etc/modprobe.d/cylance.conf`
	`/etc/init.d/cylancesvc`
	`/etc/dbus-1/system.d/com.cylance.agent_server.conf`
	`/var/run/cylancesvc.pid`
	CylanceUI:
	`/etc/xdg/autostart/cylance-protect.desktop`
	`/usr/share/applications/cylance-protect.desktop`

SUSE (SLES) 12 SP1, SP2, SP3, SP4
SUSE (SLES) 15
	CylancePROTECT:
	`/opt/cylance`
	`/usr/src/CyProtectDrv-1.2`
	`/tmp/CylanceDesktopArchive`
	`/tmp/CylanceDesktopRemoteFile`
	`/lib/modules/*/extra/CyProtectDrv.ko`
	`/etc/sysconfig/modules/cylance.modules`
	`/etc/modprobe.d/cylance.conf`
	`/usr/lib/systemd/system/cylancesvc.service`
	`/etc/dbus-1/system.d/com.cylance.agent_server.conf`
	`/var/run/cylancesvc.pid`
	Proxy configuration (only if required):
	`/etc/systemd/system/cylancesvc.service.d/proxy.conf`
	CylanceUI:
	`/etc/xdg/autostart/cylance-protect.desktop`
	`/usr/share/applications/cylance-protect.desktop`
	`/usr/share/gnome-shell/extensions/cylance-protect@cylance.com`

Linux Version	Path

Ubuntu LTS/Xubuntu 14.04	CylancePROTECT:
	`/opt/cylance`
	`/usr/src/CyProtectDrv-1.2`
	`/tmp/CylanceDesktopArchive`
	`/tmp/CylanceDesktopRemoteFile`
	`/lib/modules/*/extra/CyProtectDrv.ko`
	`/etc/modprobe.d/cylance.conf`
	`/etc/init/cylancesvc.conf`
	`/etc/dbus-1/system.d/com.cylance.agent_server.conf`
	`/var/run/cylancesvc.pid`
	Proxy configuration (only if required):
	`/etc/init/cylancesvc.override`
	CylanceUI:
	`/usr/share/applications/cylance-protect.desktop`
	`/etc/xdg/autostart/cylance-protect.desktop`

Ubuntu LTS/Xubuntu 16.04, 18.04, 20.04
Debian 10, 11
	CylancePROTECT:
	`/opt/cylance`
	`/usr/src/CyProtectDrv-1.2`
	`/tmp/CylanceDesktopArchive`
	`/tmp/CylanceDesktopRemoteFile`
	`/lib/modules/*/extra/CyProtectDrv.ko`
	`/etc/modprobe.d/cylance.conf`
	`/lib/systemd/system/cylancesvc.service`
	`/etc/dbus-1/system.d/com.cylance.agent_server.conf`
	`/var/run/cylancesvc.pid`
	Proxy configuration (only if required):
	`/etc/systemd/system/cylancesvc.service.d/proxy.conf`
	CylanceUI:
	`/usr/share/applications/cylance-protect.desktop`
	`/etc/xdg/autostart/cylance-protect.desktop`

Linux driver is not loaded. Upgrade the driver package.

Cause

The CylancePROTECT Desktop driver on the device is not compatible with the Linux kernel.

Solution

Update the Linux driver based on one of the following scenarios:

Item	Description
The device is running agent version 3.1 or later	Do one of the following: • Set the zone update rule to automatically update the Linux driver. • Manually update the Linux driver.
The device is running agent 2.1.1590 or later (up to 3.0)	• Manually update the Linux driver.

Troubleshooting CylanceOPTICS

This section provides information to help you troubleshoot and resolve issues with CylanceOPTICS.

Troubleshooting issues with the CylanceOPTICS agent on Linux

Problem	Possible solution
The kernel-header and kernel-devel packages do not match the kernel.	Use yum update kernel and restart the device. If a restart is not possible, use one of the following commands: • RHEL/CentOS or Amazon Linux 2: `` yum install kernel-headers-`uname -r` kernel-devel-`uname -r` `` • Ubuntu: `sudo apt-get install linux-headers -$(uname -r)`
If you enable debug logging, a “Corroborator found a match for PID...” message occurs in logs.	This message is expected and does not indicate a bug or other issue.

Removing the CylanceOPTICS agent from a device

When you uninstall the CylanceOPTICS agent from a device, any local data that was stored by CylanceOPTICS and log files are also removed. You must uninstall the CylanceOPTICS agent before you uninstall the CylancePROTECT agent.

To uninstall the agent, use the standard uninstall options available on the OS (for example, Add/Remove Programs on Windows or uninstall from Finder > Applications on macOS), or uninstall the CylanceOPTICS agent using the OS commands covered in the Cylance Endpoint Security Setup content.

For Windows, if you want to uninstall the agent using OS commands, the user must take ownership of the files and directories owned by the local system. If you enabled the prevent service shutdown feature for the CylanceOPTICS agent for Windows (under protection settings in the device policy), you must turn off this feature (or assign a different device policy where this feature is not enabled) before you try to remove the CylanceOPTICS agent.

It is a best practice to restart the device after you uninstall the agent.

Removing the CylanceOPTICS agent from a macOS device

Verify that the CylanceOPTICS agent has been removed

Run the following command:

```
kextstat | grep -i cyoptic
```

For macOS Big Sur (11.x), run the following command as well:

```
systemextensionsctl list | grep -i cyoptics
```

The commands should return no output.

Confirm that the following paths and files are no longer present on the system:

- /Library/Application Support/Cylance/Optics
- /Library/Application Support/OpticsUninstall
- /Applications/Cylance/Optics
- /Library/LaunchDaemons/com.cylance.cyoptics_service.plist
- /Library/LaunchDaemons/com.cylance.optics.postuninstall.plist
- /Library/LaunchDaemons/com.cylance.cyopticsesfservice.plist

On a macOS Big Sur (11.x) device, after using an ssh session to silently uninstall the CylanceOPTICS agent, /Applications/Cylance/Optics/CyOpticsESFLoader.app remains and the system extension is still active

This issue occurs because Apple has no mechanism to silently uninstall system extensions without explicit confirmation by the end user.

To resolve, use the finder to locate CyOpticsESFLoader.app and drag it to the trashcan, then confirm the UI prompt to deactivate and remove the system extension.

If you get a permissions error when you drag the file to the trashcan, run the following command to temporarily disable CylancePROTECT Desktop:

```
sudo launchctl unload /Library/LaunchDaemons/com.cylance.agent_service.plist
```

After you run the command, you can drag the file to the trashcan and confirm the UI prompt. If you want CylancePROTECT Desktop to remain active, restart the device.

Note: You must remove CyOpticsESFLoader.app in this way before removing the CylancePROTECT Desktop agent from the device. If you remove the CylancePROTECT Desktop agent before completing this task, /Applications/Cylance is removed from the device, including CyOpticsESFLoader.app, so you will not be able to manually delete it and deactivate the system extension.

Legal notice

©2024 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, CYLANCE and SECUSMART are the trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners.

Patents, as applicable, identified at: www.blackberry.com/patents.

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