



# **CylanceMDR**

## **User Guide**



# Contents

- Overview..... 4**
  - CylanceMDR requirements..... 5
  - System requirements..... 6
  - CylanceMDR On-Demand..... 7
  - Supported third-party integrations..... 7
  - Configuration and firewall settings for CylanceMDR syslog mirroring..... 8
  - Critical event management mobile app integration with CylanceMDR..... 10
  - CylanceMDR email addresses to allow..... 10
  - Onboarding and configuration..... 11
  
- Log in to the portal..... 12**
  
- Profile..... 13**
  - Reconfigure multi-factor authentication..... 13
  - Change your password..... 14
  
- Dashboard..... 15**
  
- Contacts..... 18**
  - Create a user..... 18
  - Export a list of users..... 19
  
- Escalations..... 20**
  - Searching for alerts..... 20
  - Set the priority of an alert..... 21
  - Change the assignee..... 21
  - Add comments..... 21
  - Close an alert..... 22
  
- Reports..... 23**
  - Export a report..... 23

# Overview

CylanceMDR is a subscription-based, 24x7-managed extended detection and response (XDR) service that provides actionable intelligence for customers to prevent threats quickly, while minimizing alert fatigue without requiring additional resources. This service is fully integrated with CylancePROTECT, CylanceOPTICS, CylanceGATEWAY, and third-party vendors to provide holistic and unified telemetry across all endpoints and enable highly skilled BlackBerry analysts to threat-hunt through customer environments to find and contain threats, prevent major breaches, and allow organizations to mature their security posture. BlackBerry has the strategy, expertise, and technology to protect an organization by analyzing, preventing, and containing threats as well as large-scale breaches.

CylanceMDR requires CylancePROTECT and CylanceOPTICS. CylanceGATEWAY optional for CylanceMDR Advanced subscriptions. For more information, see the [CylanceMDR requirements](#).

## What's included in the subscription

The following table highlights the features that are included in CylanceMDR Advanced, CylanceMDR Standard, and CylanceMDR On-Demand subscriptions.

The CylanceMDR Standard and Advanced subscriptions include closed-loop communications and access to a CylanceMDR analyst to help navigate incidents and provide regular updates and ongoing review of the overall threat prevention status. Optionally, customers are also eligible to secure services for third-party applications, such as for integrating and managing telemetry data from SIEM.

Feature	CylanceMDR On-Demand	CylanceMDR Standard	CylanceMDR Advanced
Onboarding (configuration and finetuning)		✓	✓
24x7 threat monitoring		✓	✓
24x7 threat detection	✓	✓	✓
24x7 triage and response	✓	✓	✓
24x7 threat hunting		✓	✓
Custom threat hunting		✓	✓
Monthly reports		✓	✓
Advisory services		✓	✓
Critical Event Management mobile app		✓	✓
Threat intelligence indicators of compromise (IOC) integration		✓	✓

Feature	CylanceMDR On-Demand	CylanceMDR Standard	CylanceMDR Advanced
24x7 phone support		✓	✓
Advanced threat intelligence (simulation, validation, monthly reports)			✓
Incident response and forensic investigation	Optional add-on	Optional add-on	✓
Service level objectives	✓	✓	✓
\$1,000,000 guarantee			(Optional)

<sup>1</sup> You must obtain a third-party solution (for example, for SIEM integration). For more information, see [Supported third-party integrations](#).

## CylanceMDR requirements

CylancePROTECT and CylanceOPTICS are required when you want to subscribe to CylanceMDR. The following table lists the products and solutions that CylanceMDR supports and highlights which are required, optional, and not applicable for CylanceMDR Advanced, CylanceMDR Standard, and CylanceMDR On-Demand subscriptions.

For example, your organization must have CylancePROTECT and CylanceOPTICS if you want to subscribe to CylanceMDR. If you want to use CylanceGATEWAY and third-party solution integrations, you must subscribe to CylanceMDR Standard or Advanced.

Product	CylanceMDR On-Demand	CylanceMDR Standard	CylanceMDR Advanced
CylancePROTECT	Required	Required	Required
CylanceOPTICS	Optional <sup>1</sup>	Required	Required
CylanceGATEWAY	Optional <sup>1</sup>	Optional <sup>1</sup>	Optional <sup>1</sup>
Third-party solution integration (for example, for SIEM integration)	N/A	Optional <sup>1</sup>	Optional <sup>1</sup>
Incident response retainer (for example, <a href="#">BlackBerry Security Services</a> )	Optional <sup>1</sup>	Optional <sup>1</sup>	Included

<sup>1</sup> If you want to integrate these features, an additional purchase may be required.

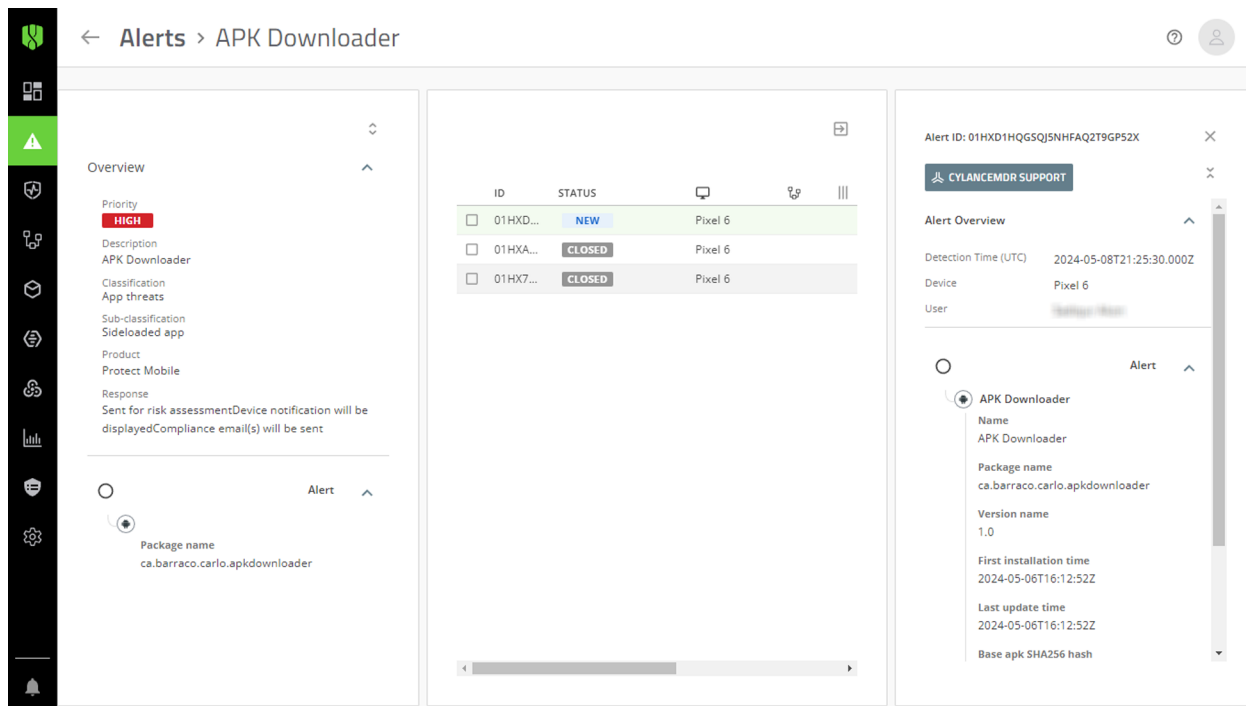
# System requirements

CylanceMDR requires the following:

- CylancePROTECT Desktop agent, CylancePROTECT Mobile app, and CylanceOPTICS agent installed on the endpoints.
- CylanceGATEWAY desktop agent installed on the endpoints.
- The latest Google Authenticator app is required to log in to the CylanceMDR (CylanceGUARD) portal using multi-factor authentication (MFA).

Requirement	Description
Agent and operating system versions	<p>It is recommended that you run the latest version of the agent that's supported for your OS with the CylanceMDR solution. See the OS compatibility matrix content for each of the agents:</p> <ul style="list-style-type: none"><li>• <a href="#">CylancePROTECT Desktop compatibility matrix</a></li><li>• <a href="#">CylancePROTECT Mobile compatibility matrix</a></li><li>• <a href="#">CylanceOPTICS compatibility matrix</a></li><li>• <a href="#">CylanceGATEWAY compatibility matrix</a></li></ul> <p>For software and hardware requirements for each of the agents, <a href="#">see the requirements content</a>.</p> <p>For information about the software lifecycle for BlackBerry enterprise products, see the <a href="#">BlackBerry Enterprise Software Lifecycle Reference Guide</a>.</p>
Data storage and collection	<p>CylanceMDR collects data that is natively collected by CylancePROTECT and CylanceOPTICS. Potential forensic data sets may be collected in the case of an incident. Data collection includes information contained in both CylancePROTECT and CylanceOPTICS alerts as well as data captured through the Package Deploy (Refract) and InstaQuery. Package Deploy has the ability to pull forensic artifacts from the file system at almost any level, while InstaQuery returns filesystem, registry, process, and network information from the customer environment.</p>

# CylanceMDR On-Demand



The CylanceMDR On-Demand subscription is a convenient and helpful option if your organization monitors the alerts that are reported to the Cylance console. With this subscription, you can request CylanceMDR support on demand for any alerts that you think might be a threat but you need the time and expertise of a CylanceMDR analyst to help you resolve it. You can request support from an alert in an alert group in the Alerts view in the Cylance console. CylanceMDR analysts are immediately notified with the alert details and can start their investigation and assess the threat. To track and follow up on the investigation (for example, to share additional details), you can log in to the CylanceMDR (CylanceGUARD) portal and find the alert in the Escalations screen.

## Supported third-party integrations

When you integrate CylanceMDR with third-party vendors for managed XDR services, you unify endpoint detection and response (EDR) with other security and business tools for improved visibility and control of security incidents across the business in a single unified console. Related telemetry data from various tools across the environment are automatically associated with a single incident, reducing the manual effort and unnecessary context switching. Based on the efficacy, correlation, and actions of incidents from the various telemetry sources, CylanceMDR can be optimized to automatically take action against security incidents in real-time.

A CylanceMDR Advanced subscription is required to support third-party integrations.

The following table lists the supported third-party solutions that can be integrated with CylanceMDR.

Solution	Supported third-party integrations
<p><b>Security Incident and Event Management (SIEM)</b>            technology supports threat detection, compliance, and security incident management through the collection and analysis (both near real-time and historical) of security events, as well as a wide variety of other event and contextual data sources.</p>	<ul style="list-style-type: none"> <li>• <a href="#">Exabeam</a></li> </ul>

## Configuration and firewall settings for CylanceMDR syslog mirroring

To allow communication between BlackBerry syslog mirroring servers and your organization's syslog servers, you need to configure your organization's firewall to allow connections from the appropriate BlackBerry IP addresses. Additionally, you need the FQDN (or IP) address and port of your organization's syslog servers, which needs to present a signed, TLS-enabled, server certificate to receive syslog messages. If your organization requires mTLS authentication, you need to provide a signed client certificate to BlackBerry. The following table lists the configuration details, such as the IP addresses that you should allow based on your assigned region for the Cylance Endpoint Security management console, as well as information about how to generate an mTLS client certificate for BlackBerry.

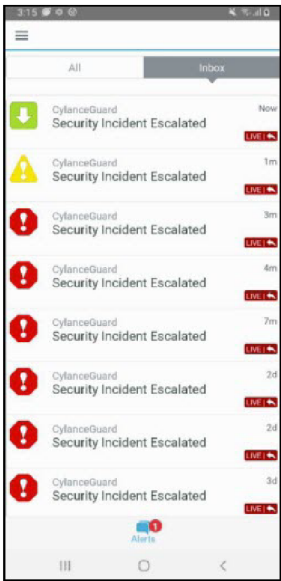
For assistance with setting up syslog mirroring for your organization, visit <https://myaccount.blackberry.com/> and open a case for CylanceMDR. A CylanceMDR analyst will work with your organization to complete the configuration.

Requirement	Description
Allow the source IP address (from BlackBerry)	Based on your assigned region, configure your firewall to allow connections from the appropriate IP address from BlackBerry: <ul style="list-style-type: none"> <li>• US: 52.202.215.1</li> <li>• EU: 52.29.124.76</li> <li>• JP: 35.73.65.169</li> <li>• AU: 54.206.75.195</li> <li>• SA: 54.232.154.173</li> </ul>
Destination address and port number	You need the FQDN (or IP) address and port number of your organization's syslog server that will receive the syslog messages. A signed, TLS-enabled, server certificate is required to establish a connection for syslog mirroring.
Protocol	TLS encrypted syslog over TCP



Requirement	Description
mTLS authentication (optional)	<p>If mTLS authentication is required for your organization, you need to generate an mTLS client certificate and provide it to BlackBerry.</p> <p>When generating the mTLS client certificate:</p> <ul style="list-style-type: none"> <li>• Use the certificate signing request (.csr) that BlackBerry provides to your organization.</li> <li>• Verify that TLS Web Server Authentication and TLS Web Client Authentication are present when signing the client certificate. Also, use the same certificate authority as your organization's syslog server.</li> </ul> <pre data-bbox="509 596 1370 705">#example command to generate a mTLS client certificate openssl x509 -req -CA rootCA.crt -CAkey rootCA.key -in blackberry.csr -out blackberry.crt -days 3650</pre>
Processing the header of the forwarded syslog event	<p>Syslog events that are forwarded to your organization's syslog servers have an extra header, in addition to the header of the original event. The header for the original event provides the accurate date and time of the event. You can configure your organization's system to process the extra header, which has the date and time of when the message was forwarded.</p> <p>The extra header is in RFC5424 format and is bolded in the example below:</p> <pre data-bbox="509 995 1414 1136"><b>2022-09-08T00:25:00.000Z 11.11.111.11 CylancePROTECT[-]:</b> 1138 &lt;44&gt;1 2022-09-08T00:24:57.000000+00:00 sysloghost CylancePROTECT - - [5555abcd-abcd-wxyz-a123-12345abcdef] Event Type: NetworkThreat, Event Name: blocked connection, Eco Id: AbC/AaaaaaBBBcc0DeFGhIJ=, User: ...</pre> <p>Prior to the November 2022 update, the extra header was in RFC3164 format and is bolded in the example below:</p> <pre data-bbox="509 1262 1414 1402"><b>&lt;13&gt; Sep 08 00:25:00 11.11.111.11 CylancePROTECT[-]:</b> 1138 &lt;44&gt;1 2022-09-08T00:24:57.000000+00:00 sysloghost CylancePROTECT - - [5555abcd-abcd-wxyz-a123-12345abcdef] Event Type: NetworkThreat, Event Name: blocked connection, Eco Id: AbC/AaaaaaBBBcc0DeFGhIJ=, User: ...</pre>

# Critical event management mobile app integration with CylanceMDR



CylanceMDR users can receive notifications through the BlackBerry AtHoc mobile app when a security incident is escalated to their organization. The AtHoc mobile app is another channel from which users can be notified as soon as possible of any incidents that require attention. From the app, users can quickly access the CylanceMDR portal from their mobile device and learn more about the incidents.

You can request critical event management integration to be enabled for your CylanceMDR organization. When it is enabled, CylanceMDR users receive a Welcome email with information about how to download and register the AtHoc mobile app. For more information, see [Register the BlackBerry AtHoc mobile app for the CylanceMDR service](#).

After a user registers the AtHoc mobile app on the device, they receive app notifications when a security incident is escalated to them. For more information, see [Responding to CylanceMDR alerts in the AtHoc mobile app](#).

## CylanceMDR email addresses to allow

You can expect to receive email messages from CylanceMDR and analysts. To prevent the email messages from being blocked or marked as spam, it is recommended that your email software is configured to allow messages from the certain addresses and domains. The following table lists the email addresses and domains that you should allow:

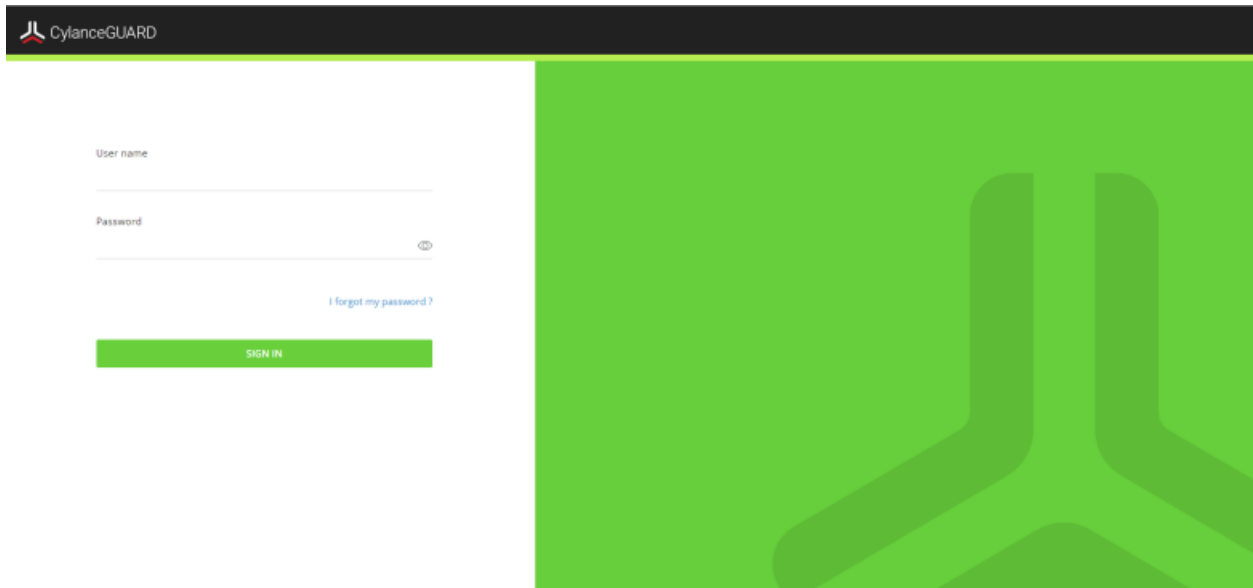
Email address or domain	Description
admin@portal.cylance.io	This email address is used for email notifications from the Cylance Endpoint Security management console, such as invitations and escalations for CylancePROTECT and CylanceOPTICS.

Email address or domain	Description
noreply@blackberry.com	This email address is used for email notifications from CylanceMDR, such as invitations and onboarding email messages.
*.blackberry.com	You may receive email messages, such as reports, from analysts that have an email address in this domain.
*.service-now.com	You may receive automated email messages, such as incident escalation notifications, from CylanceMDR that have an email address in this domain.

## Onboarding and configuration

CylanceMDR is deployed through a proven onboarding process led by a ThreatZero expert while leveraging CylancePROTECT, CylanceOPTICS, and CylanceGATEWAY agent technology. When the deployment process is complete, you are granted access to a transparent web portal where you can manage threats to the environment.

# Log in to the portal



When you are invited to use the CylanceMDR (CylanceGUARD) portal, you receive an email with login information. Click the link in the email and follow the instructions on the screen to set a new password and set up multi-factor authentication using the Google Authenticator app to complete the registration process. The authenticator app is used to generate a multi-factor code that is required each time you log in to the CylanceMDR portal.

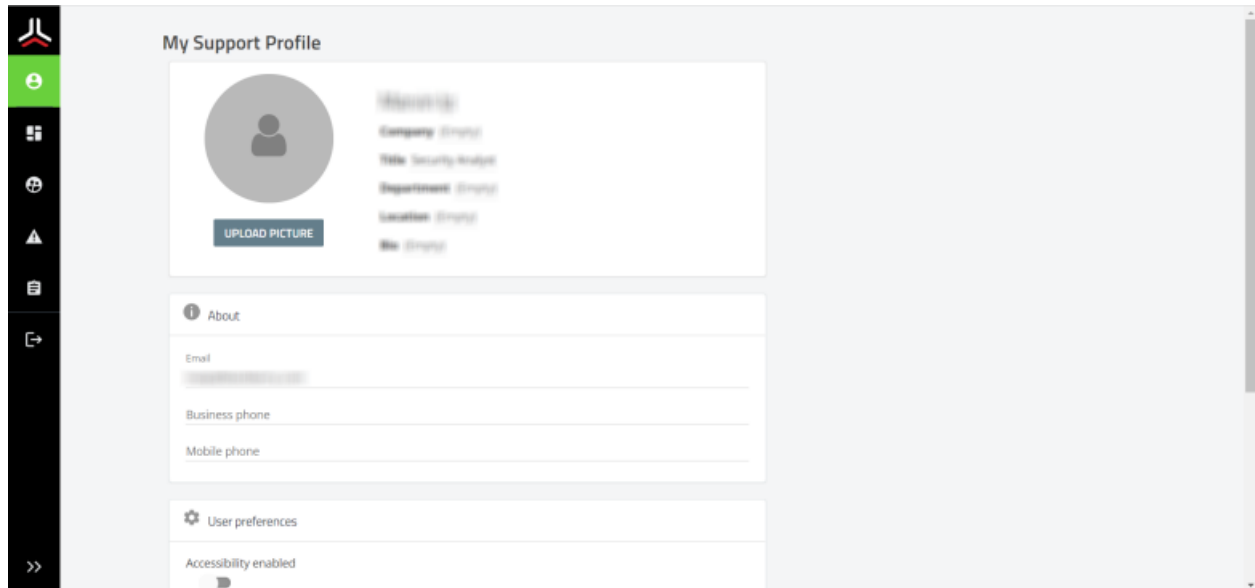
Before any of your organization's users can access the CylanceMDR portal, an administrator in your organization must log in and accept the relevant end user license agreements: the BlackBerry Solution License Agreement and the Professional Services Agreement.

**Before you begin:** You must download and install an authenticator app, such as Google Authenticator, on your mobile device.

1. Click the portal link in the email invitation.
2. Enter your username and password.
3. If prompted, change and confirm your password.
4. Enter the six-digit code displayed in the authenticator app. If you're logging in for the first time, follow the instructions on the screen to set up multi-factor authentication.
  - a) On your mobile device, open the Google Authenticator app.
  - b) Tap **+ > Scan a QR code** to scan the QR code that is displayed on the screen.
  - c) On your computer, in the **6-digit code** field, enter the code that the authenticator app generated.
  - d) Tap **Pair device and login**.
5. If it is displayed, read the **BlackBerry Solution License Agreement** and the **Professional Services Agreement** and select the checkbox to agree to them.

The portal dashboard opens. You are logged in.

# Profile



On the Profile screen, you can fill in your user profile to add information about yourself, including contact information. You can do the following:

- Set your location
- Fill in your bio
- Add contact information such as email and phone numbers
- Enable accessibility
- Set your time zone
- Reconfigure multi-factor authentication
- Change your password

## Reconfigure multi-factor authentication

When you reconfigure multi-factor authentication, you can generate new codes and invalidate codes that are generated on previously-configured devices (for example, if your device was lost or stolen), or you can add other devices that will generate the same code.

If you are trying to log in and you have lost access to your device that you already configured with multi-factor authentication, click the **Click here to receive a one time code via email** option at the top of the **2-Factor Authentication** screen. After you log in, you can follow these steps to reconfigure it.

**Before you begin:** You must download and install an authenticator app, such as Google Authenticator, on your mobile device.

1. On the menu, click **Profiles**.
2. In the **User preferences** section, click **Configure Multi-Factor Authentication**.  
A dialog with a QR Code appears.
3. Do one of the following:
  - If you want to generate new codes and invalidate codes that are generated on previously configured devices (for example, if your device was lost or stolen), click **Generate a new code** and **OK** to confirm.

- If you want to keep codes generated on previously-configured devices valid and add another device that will generate the same code, skip this step.
4. Follow the instructions on the screen to configure multi-factor authentication:
    - a) On your mobile device, open the Google Authenticator app.
    - b) Tap **+** > **Scan a QR code** to scan the QR Code that is displayed on the screen.
    - c) If you chose to generate new codes, enter the new code and tap **Pair device**.

At the top of the dialog box, a **Multi-factor authentication has been successfully configured** message displays in green.

## Change your password

1. On the menu, click **Profiles**.
2. In the **Security** section, click **Change Password**.
3. In the **Current Password** field, enter your current password.
4. In the **New password** field, enter your new password.
5. In the **Confirm password** field, confirm your new password.
6. Click **Change**.

# Dashboard

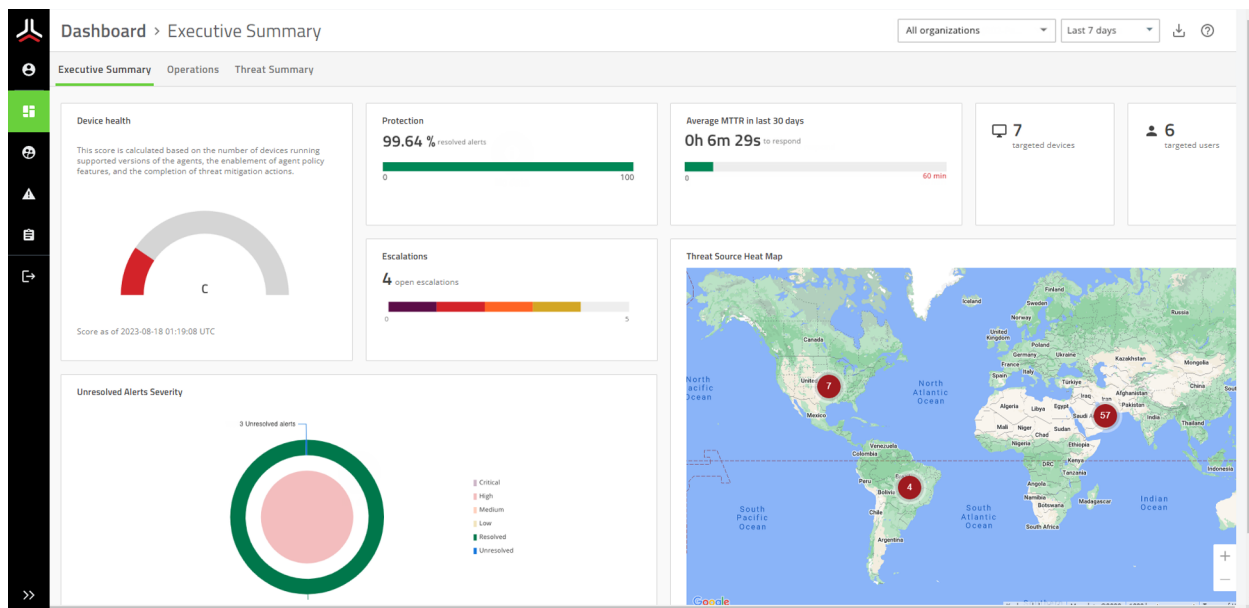
The CylanceMDR Dashboard page has an interactive layout that visually displays the various types of alerts that were escalated in your organization, as well as top threats by alert type or target.

You can set the timeframe to limit the data that is presented on the dashboard. For example, you can limit the data to the last 24 hours so that you view only a list of escalations that occurred in that timeframe. If you manage multiple child organizations, you can also limit the results to specific organizations. These settings can be found on the top right of the Dashboard page. If there is no data available according to the specified timeframe, the widget will display "No data".

The following dashboard views are available out of the box:

- **Executive Summary:** This view provides a high level view of the overall protection status and threat landscape, such as visualizations of open and resolved alerts, as well as a map of threat sources.
- **Operations:** This view provides a quick report of the open escalations and top types of threats allowing users to target high-priority threats and resolve them as soon as possible.
- **Threat Summary:** This view provides a quick report of the number of incidents, escalated incidents, open escalations, and the top rules that were applied to fewest devices, allowing users to see the effectiveness of their threat strategy and take necessary actions.

## Executive Summary dashboard

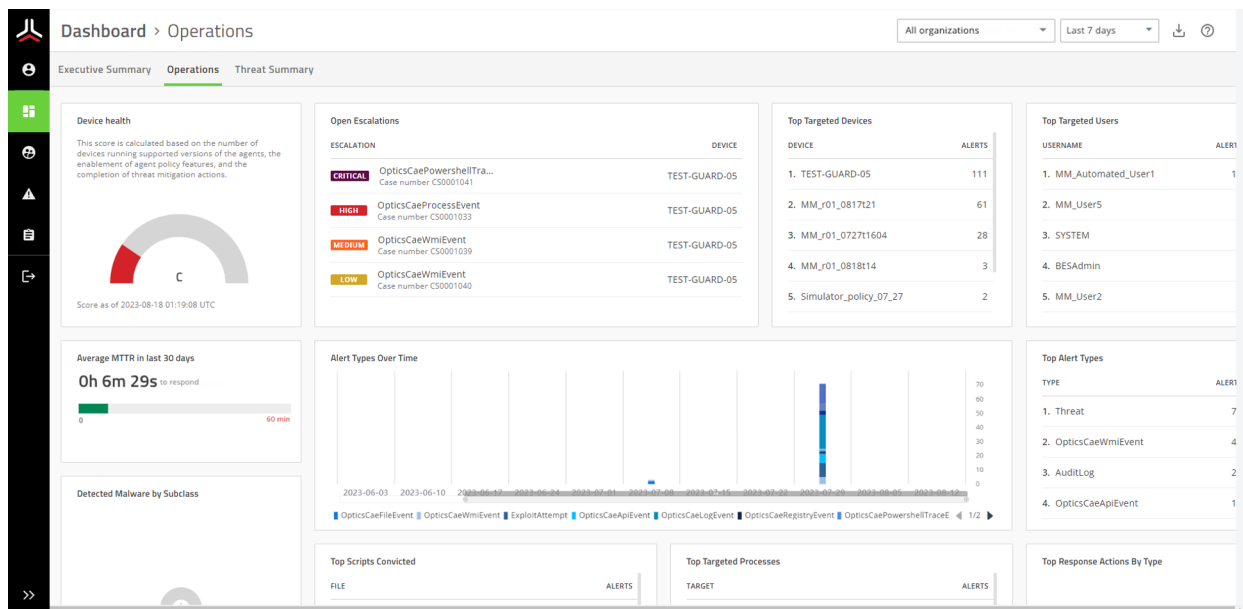


The following alert metrics are displayed in the Executive Summary tab of the dashboard:

- **Device health:** View a score that is calculated based on the number of devices running supported versions of the Cylance agents, the enablement of agent policy features, and the completion of threat mitigation actions.
- **Protection:** View the current percentage of alerts that are resolved.
- **Escalations:** View a graph of escalations to see the ratio of unresolved threats by severity, as well as threats that were already resolved. You can click on parts of this widget to view a list of all open escalations, or view a list of open escalations of a specific severity. Escalations are alerts that are brought to the attention of your organization.
- **Average MTTR in last 30 days:** View the average time for analysts to escalate and close alerts in the last 30 days.

- **Targeted users:** View the number of users that were targeted.
- **Targeted devices:** View the number of devices that were targeted.
- **Unresolved Alerts Severity:** View a graph that shows the status of overall alerts by severity. At a glance, you can see the ratio of resolved and unresolved alerts. Unresolved alerts are incoming alerts that CylanceMDR analysts are working on that may or may not be escalated to your organization for attention.
- **Threat Source Heat Map:** View a map of threat sources to understand where attacks are originating from. You can click the numbers that appear on the map to see the severity of threats for each geographic area.

## Operations dashboard

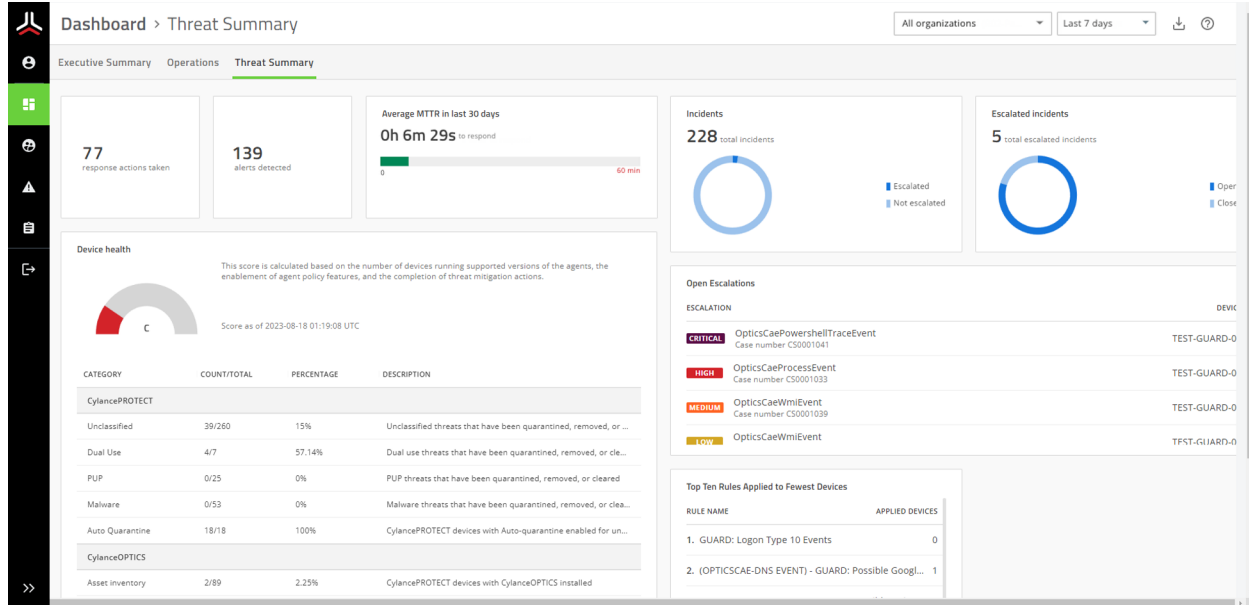


The following alert metrics are displayed in the Operations tab of the dashboard:

- **Device health:** A score that is calculated based on the number of devices running supported versions of the Cylance agents, the enablement of agent policy features, and the completion of threat mitigation actions.
- **Average MTTR in last 30 days:** View the average time for analysts to escalate and close alerts in the last 30 days.
- **Open Escalations:** View a list of open escalations that might require your attention, such as those with critical and high severity. You can click on an alert to quickly jump to its details.
- **Top Alert Types:** View the top alert types to see the alert types (such as memory exploit attempts, script control threats, and network threats) that are reported most frequently in your organization.
- **Detected Malware by Subclass:** View the top malware types by subclass, such as whether a threat was a trojan, virus, or worm.
- **Top Scripts Convicted:** View the top scripts to see the scripts that are run the most often in your organization that are also generating alerts. Hover over a script in the list to see the full directory path to the script.
- **Alert Types Over Time:** View the top alert types that have occurred over a period of time. You can adjust the timeframe by sliding the bar below the x-axis and click the alert types to show or hide them in the graph.
- **Top Targeted Processes:** View the top targeted processes to see the processes that are most often targeted by threats.
- **Top Targeted Devices:** View the top targeted devices to see the devices that are generating the most alerts.
- **Top Targeted Users:** View a list of users that have encountered the most threats.
- **Top Response Actions By Type:** View a list of the top response actions that were used to resolve threats.



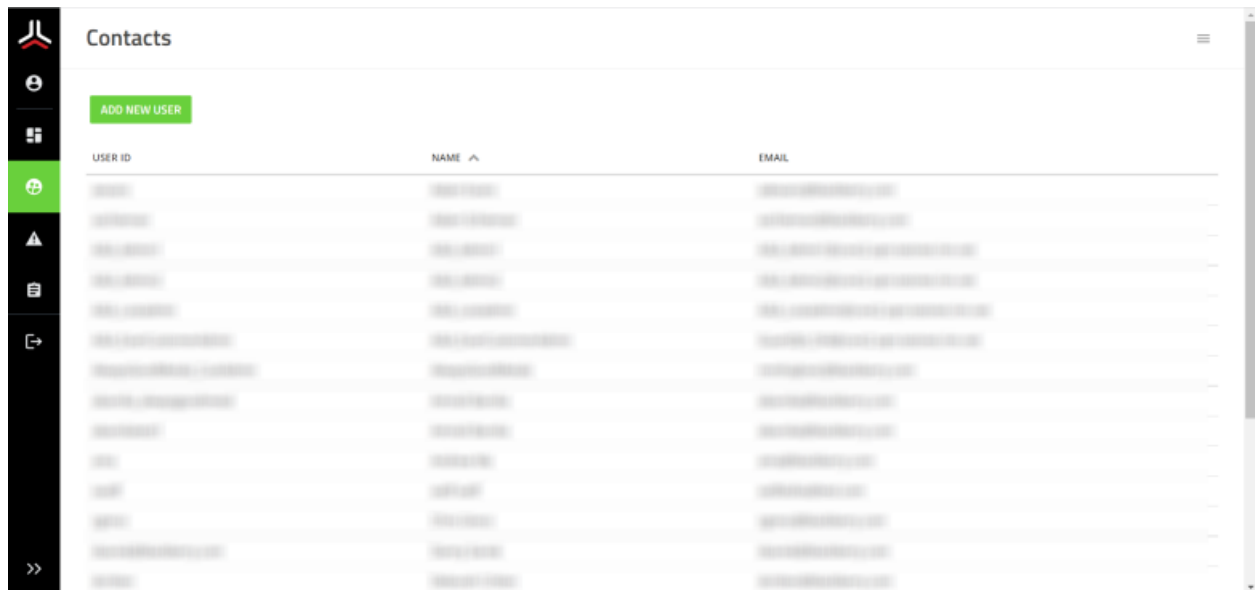
## Threat Summary dashboard



The following alert metrics are displayed in the Operations tab of the dashboard:

- **Response actions taken:** The number of actions taken within the specified timeframe.
- **Alerts detected:** The number of alerts detected within the specified timeframe.
- **Average MTTR in last 30 days:** View the average time for analysts to escalate and close alerts in the last 30 days.
- **Incidents:** View the total number of incidents that were escalated and not escalated.
- **Escalated incidents:** View a list of incidents that were recently escalated.
- **Device health:** A score that is calculated based on the number of devices running supported versions of the Cylance agents, the enablement of agent policy features, and the completion of threat mitigation actions.
- **Open Escalations:** View a list of open escalations that might require your attention, such as those with critical and high severity. You can click on an alert to quickly jump to its details.
- **Top Ten Rules Applied to the Fewest Devices:** View a list of CylanceOPTICS rules that were applied to the fewest devices.

# Contacts



On the Contacts page, administrators in an organization can add and manage their CylanceMDR users. They can also export a list of users in PDF, CSV, and Excel format.

## Create a user


If you are an administrator of an organization, you can add users so that they can use the CylanceMDR portal. If you manage multiple organization accounts in CylanceMDR, you can select the organization that the user can access (if you select a parent organization, they can also access its child organizations).

If you want to create an administrator, you must contact BlackBerry Support.

1. On the menu, click **Contacts**.
2. Click **Create New User**.
3. Enter the following required information:
  - User ID
  - Account
  - First Name
  - Last Name
  - Email address
4. Optionally, enter the following information.
  - Business Phone
  - Mobile Phone
  - Title
  - Language
5. Click **Submit**.

**After you finish:** The user receives an email invitation to access the CylanceMDR portal. They must follow the instructions in the email message to complete the registration.

## Export a list of users

1. On the menu, click **Contacts**.
2. Click  and do one of the following:
  - Click **Export as PDF**.
  - Click **Export as Excel**.
  - Click **Export as CSV**.
3. Save the file to your computer.

# Escalations


CASE NUMBER	ARTIFACT OF INTEREST	HOST/ DEVICE NAME	PRIORITY	SEVERITY ↑	TRIGGER PRODUCT	ASSIGNED TO	TIMESTAMP	STATUS	O
CS0001420	LoginSuccess		P5	Critical	AuditLog		2022-10-20 19:09:01	New	Q
CS0001111	threat_found	HL_400006_FakeDevice_391230407784037884...		Critical	Protect		2022-05-26 15:00:57	Closed	A
CS0001112	Blocked	HL_400006_FakeDevice_107504207874037884...		Critical	Protect		2022-05-26 15:04:47	Closed	A
CS0001113	Alert	HL_400006_FakeDevice_107504207874037884...		Critical	Protect		2022-05-26 15:04:47	Closed	A
CS0001114	allowed	HL_400006_FakeDevice_107504207874037884...		Critical	Protect		2022-05-26 15:04:47	Closed	A

An alert is a collection of events that are correlated into a single incident. The Escalations page provides users details and access to the triggering events captured from CylancePROTECT and CylanceOPTICS. Each alert that was escalated displays as a separate escalation on this page and can be assigned to you or another group member. You can add comments to escalations to communicate with CylanceMDR analysts about the threat.

If your organization is subscribed to CylanceMDR Standard or Advanced, analysts monitor your alerts for you and will escalate them to you if they require your attention. When an analyst identifies a threat and escalates it in your organization, designated groups in your organization are notified and you can view them on the Escalations page.

If your organization is subscribed to CylanceMDR On-Demand, you must manually request CylanceMDR support from the Alerts page in the Cylance console. These requests are escalated to CylanceMDR analysts so that they can investigate. You can follow up on these requests from the Escalations page in the CylanceMDR (CylanceGUARD) portal.

On the Escalations page, you can do the following:

- Click an alert or escalation in the list to view its details.
- Enter keywords in the search field to filter the alerts.
- For advanced search, click .

## Searching for alerts

On the Escalations page, you can quickly filter the results by organization, search for keywords, or apply specific search filters. For example, specify multiple search filters such as hostname, username, domain, comment, timestamp, and many other attributes.

**Filter by organization:** If your organization has parent or child accounts associated with it, you can select an organization from the list to filter it by organization.

**Keyword search:** Type some keywords in the search bar to quickly apply a keyword filter.

**Add search filters:** Click  to add search filters and specify a set of conditions that must be met. If you want to add an alternative set of criteria, you can click **New Criteria**. Click **Run** to start the search and display the results.

**Save search filters:** To save a search filter for later use, click **Save Filter**. Specify a name for the filter and its visibility.

**Load search filters:** To load a search filter that was saved, click **Load Filter** and click the search filter that you want. You can also delete a search filter from here.


**Sort search filters:** You can click **Add Sort** to sort the results according to a specific field. You can also click the column headings in the search results to sort the results in ascending or descending order.

**Clear search filters:** To remove all search criteria, click **Clear All**.

**Filter out results:** To quickly hide alerts that have a specific value, right-click the value that's displayed on the screen and select **Filter Out**. For example, if you see alerts listed with several priority levels, you can use this option to hide alerts with the "P5" priority from the results.


**Show matching results only:** To quickly see alerts that have a specific value only, right-click the value that's displayed on the screen and select **Show Matching**. For example, if you see several devices listed in the results, you can use this option to show the alerts that are related to the "Windows\_PC\_123ABC" device only.

## Set the priority of an alert

1. Open the details view of an alert.
2. Beside **Priority**, click .
3. Select the priority that you want to set for the alert.
4. Click **Save**.

## Change the assignee

From an alert details page, you can assign an alert to other individuals within the currently assigned group. Both the original and new assignee are notified.

1. Open the details view of an alert.
2. Beside **Assignee**, click .
3. Select the user that you want to assign the alert to.
4. Click **Save**.

## Add comments


You can add comments when you view the details of an alert. Use comments to share useful information and note the actions that need to be taken to resolve the threat. Comments in the conversation are shown in reverse chronological order. When you add comments, CylanceMDR sends email notifications.

1. On the menu, click **Escalations**.
2. Click the alert that you want to add a comment to.
3. On the right pane, in the **Activity** tab, type your comment in the **Comments** box.
4. If you want to attach a file, click **Add attachments** and select the file that you want to add.
5. Click **Send**.

The comment is added to the conversation and the text box is cleared.

## Close an alert

You can close an alert when your organization considers it to be resolved or when no further action is required. You can also [leave a comment](#) for a CylanceMDR analyst to let them know that it can be closed. When an alert is closed, it cannot be reopened.

1. Open the details view of an alert.
2. Beside **Status**, click .
3. Select **Closed**.
4. Click **Save**.

# Reports

EVENT TYPE ↑	COMPANY	CLOSED
AuditLog	SECURE	2022-10-06 09:29:01
AuditLog	SECURE (All Organizations Only, None)	2022-10-17 08:48:45
AuditLog	SECURE	2022-10-06 09:29:17
AuditLog	SECURE	2022-10-06 09:29:18
AuditLog	SECURE	2022-10-06 09:29:18

Rows 1 - 5 of 457

CASE NUMBER ↑	HOST/ DEVICE NAME	ARTIFACT OF INTEREST	COMPANY	TIMESTAMP	PRIORITY	CATEGORY
CS0001019	192.168.1.100	threat_found	SECURE	2021-11-10 16:22:15	Low	Issue


The Reports page displays more detailed alert metrics for your organization. Beside each alert metric, you can choose to export a report in XLS, CSV, or PDF format.

The following are some examples of reports that are displayed on this dashboard:

- Closed alerts by event trigger type
- Escalated alerts detail
- User last login

## Export a report

CylanceMDR exports the results that are currently displaying on the Reports screen. For example, if multiple organizations are associated with your organization account, you can select a child organization to filter the results and export the reports for it. If no specific organizations are selected, the results for all organizations that you manage are displayed.

1. On the menu, click **Reports**.
2. If necessary, select the organizations that you want to filter the reports for and click **Apply**. The filter is applied and the reports on the page are refreshed.
3. Beside the report that you want to export, click  and do one of the following:
  - Click **Export as PDF**.
  - Click **Export as Excel**.
  - Click **Export as CSV**.
4. Save the file to your computer.