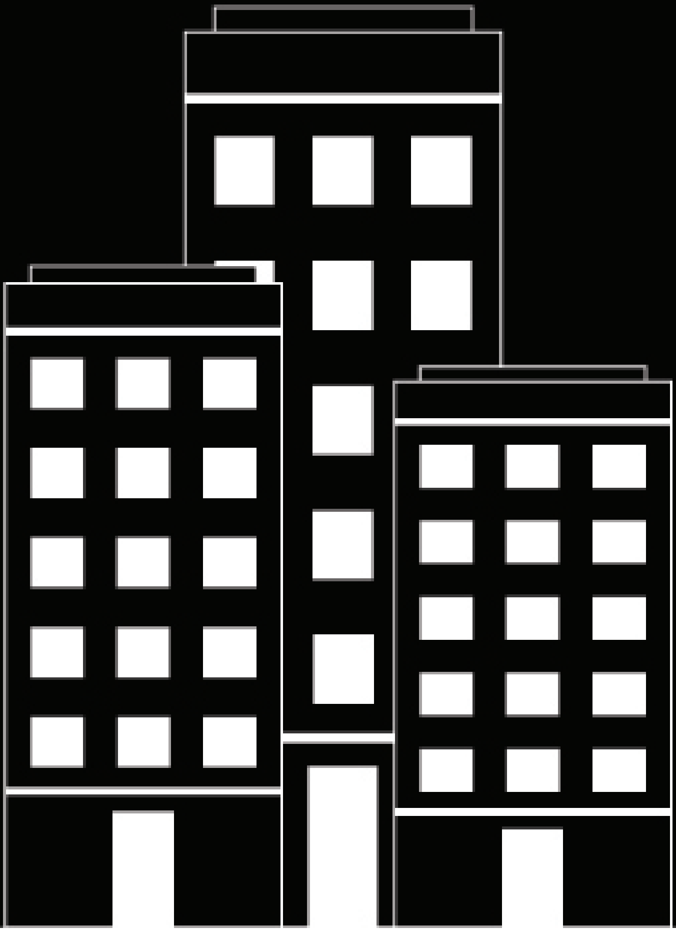


CylanceMDR

User Guide

Contents

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, and CylanceGATEWAY and can be integrated with third-party vendors to provide holistic and unified telemetry across all endpoints. Highly skilled BlackBerry analysts 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, but with the CylanceMDR Pro subscription, you can use your current endpoint protection, detection, and response solutions. CylanceGATEWAY is optional. For more information, see the CylanceMDR requirements.

What's included in the subscription

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

The CylanceMDR Standard, Advanced, and Pro 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. For CylanceMDR Pro subscriptions, third-party application integration is available, such as for firewall integration. For CylanceMDR On-Demand subscriptions, support is provided on demand only.

Feature	CylanceMDR On-Demand	CylanceMDR Standard	CylanceMDR Advanced	CylanceMDR Pro
Onboarding (Alert finetuning and Cylance product configuration)		√	√	√[1]
24x7 threat monitoring		√	√	√
24x7 threat detection	√	√	√	√
24x7 triage and response	√	√	√	√
24x7 threat hunting		√	√	√
Custom threat hunting		√	√	√
Monthly reports		√	√	√
Advisory services		√	√	√

Feature	CylanceMDR On-Demand	CylanceMDR Standard	CylanceMDR Advanced	CylanceMDR Pro
Critical Event Management mobile app		√	√	√
Threat intelligence indicators of compromise (IOC) integration		√	√	√
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			Eligible[2]	Eligible[2]
Third-party log source integration (for example, firewall integration)				√

[1] Alert finetuning is included but configuration is available for Cylance products only. Cylance products are optional for CylanceMDR Pro subscriptions.

[2] For information about eligibility requirements, see CylanceMDR $1 Million Guarantee.

CylanceMDR requirements

The following table lists the products and solutions that CylanceMDR supports and highlights which are required, optional, and not applicable for CylanceMDR On-Demand, CylanceMDR Standard, CylanceMDR Advanced, and CylanceMDR Pro subscriptions.

For example, your organization must have CylancePROTECT and CylanceOPTICS if you want to subscribe to CylanceMDR Standard or Advanced. If your organization wants CylanceMDR to receive and monitor alerts from third-party integrations such as firewall, email gateway, and cloud providers, you must subscribe to CylanceMDR Pro.

Product	CylanceMDR On-Demand	CylanceMDR Standard	CylanceMDR Advanced	CylanceMDR Pro
CylancePROTECT	Required	Required	Required	Optional[1]
CylanceOPTICS	Optional[1]	Required	Required	Optional[1]
CylanceGATEWAY	Optional[1]	Optional[1]	Optional[1]	Optional[1]
Third-party technology integration (for example, firewall integration)	N/A	N/A	N/A	Optional[1]

[1] If you want to integrate these features, an additional purchase may be required.

System requirements

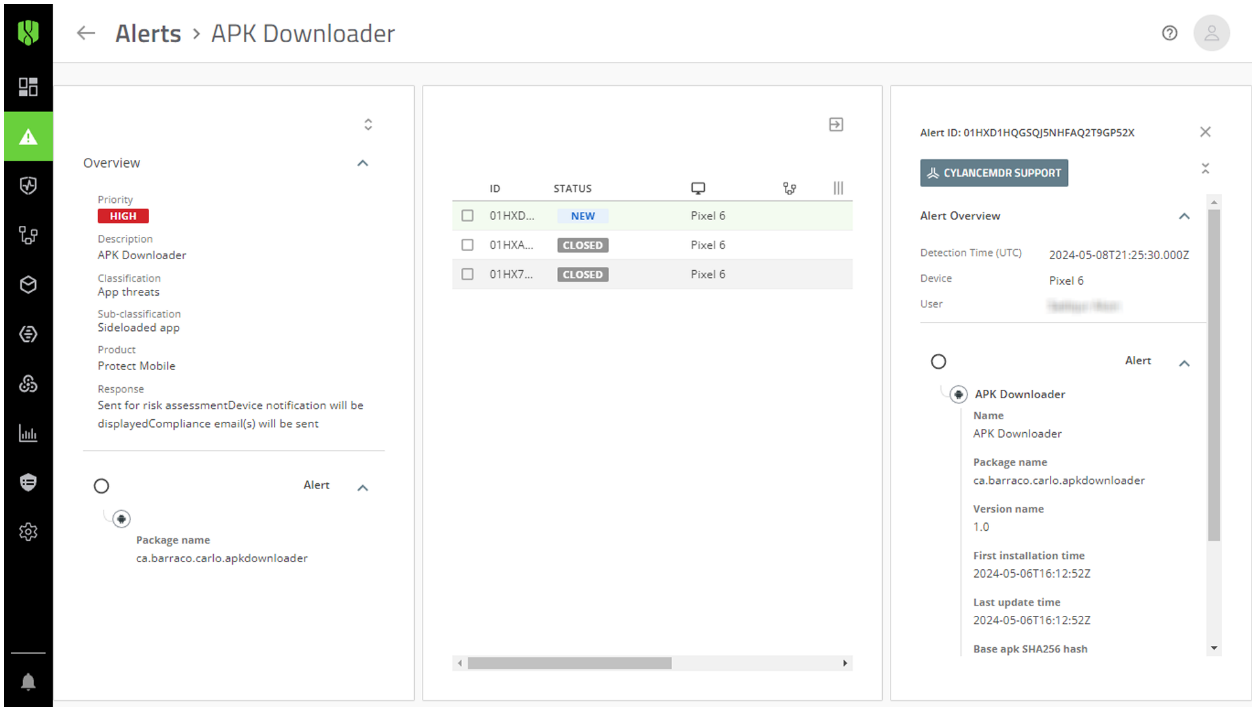
CylanceMDR requires the following:

- 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	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: • CylancePROTECT Desktop compatibility matrix • CylancePROTECT Mobile compatibility matrix • CylanceOPTICS compatibility matrix • CylanceGATEWAY compatibility matrix For software and hardware requirements for each of the agents, see the requirements content. For information about the software lifecycle for BlackBerry enterprise products, see the BlackBerry Enterprise Software Lifecycle Reference Guide.

Requirement	Description
Data storage and collection	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.

CylanceMDR On-Demand



Alerts > APK Downloader

Overview

Priority
HIGH

Description
APK Downloader

Classification
App threats

Sub-classification
Sideloaded app

Product
Protect Mobile

Response
Sent for risk assessmentDevice notification will be displayedCompliance email(s) will be sent

Alert

Package name
ca.barraco.carlo.apkdownloader

	ID	STATUS	
□	01HXD...	NEW	Pixel 6
□	01HXA...	CLOSED	Pixel 6
□	01HX7...	CLOSED	Pixel 6

Alert ID: 01HXD1HQGSQJ5NHFAQ2T9GP52X

CYLANCEMDR SUPPORT

Alert Overview

Detection Time (UTC) 2024-05-08T21:25:30.000Z

Device Pixel 6

User [redacted]

Alert

APK Downloader

Name
APK Downloader

Package name
ca.barraco.carlo.apkdownloader

Version name
1.0

First installation time
2024-05-06T16:12:52Z

Last update time
2024-05-06T16:12:52Z

Base apk SHA256 hash

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 CylanceMDR support from an alert in an alert group in the Alerts view in the Cylance console. CylanceMDR analysts are immediately notified of the escalation with the alert details and can start their investigation and assess the threat. You can track and follow up on the investigation (for example, to share additional details) from the Incidents screen.

Integrating third-party log sources with CylanceMDR Pro

When you integrate third-party log sources with CylanceMDR, 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 console. Related telemetry data from various tools across the environment are automatically associated with a single incident, reducing 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 Pro subscription is required to support the integration of third-party log sources.

For more information about integrating third-party log sources with CylanceMDR so that suspicious activities can be reported and tracked from the Cylance console, see Integrating third-party log sources.

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.

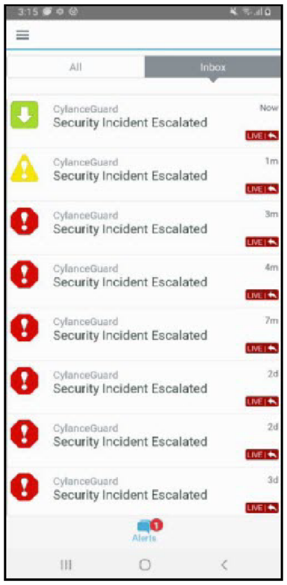
Requirement	Description
Allow the source IP address (from BlackBerry)	Based on your assigned region, configure your firewall to allow connections from the appropriate IP address from BlackBerry: • US: 52.202.215.1 • EU: 52.29.124.76 • JP: 35.73.65.169 • AU: 54.206.75.195 • SA: 54.232.154.173
Destination 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)	If mTLS authentication is required for your organization, you need to generate an mTLS client certificate and provide it to BlackBerry.
	When generating the mTLS client certificate:
	• Use the certificate signing request (.csr) that BlackBerry provides to your organization.
	• 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.
	`#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`

Processing the header of the forwarded syslog event	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. The extra header is in RFC5424 format and is bolded in the example below: **`2022-09-08T00:25:00.000Z 11.11.111.11 CylancePROTECT[-]:`** `1138 <44>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: …` Prior to the November 2022 update, the extra header was in RFC3164 format and is bolded in the example below: **`<13> Sep 08 00:25:00 11.11.111.11 CylancePROTECT[-]:`** `1138 <44>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: …`

Critical event management mobile app integration with CylanceMDR



CylanceGuard
Security Incident Escalated
Now
LIVE

CylanceGuard
Security Incident Escalated
1m
LIVE

CylanceGuard
Security Incident Escalated
3m
LIVE

CylanceGuard
Security Incident Escalated
4m
LIVE

CylanceGuard
Security Incident Escalated
7m
LIVE

CylanceGuard
Security Incident Escalated
2d
LIVE

CylanceGuard
Security Incident Escalated
2d
LIVE

CylanceGuard
Security Incident Escalated
3d
LIVE

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

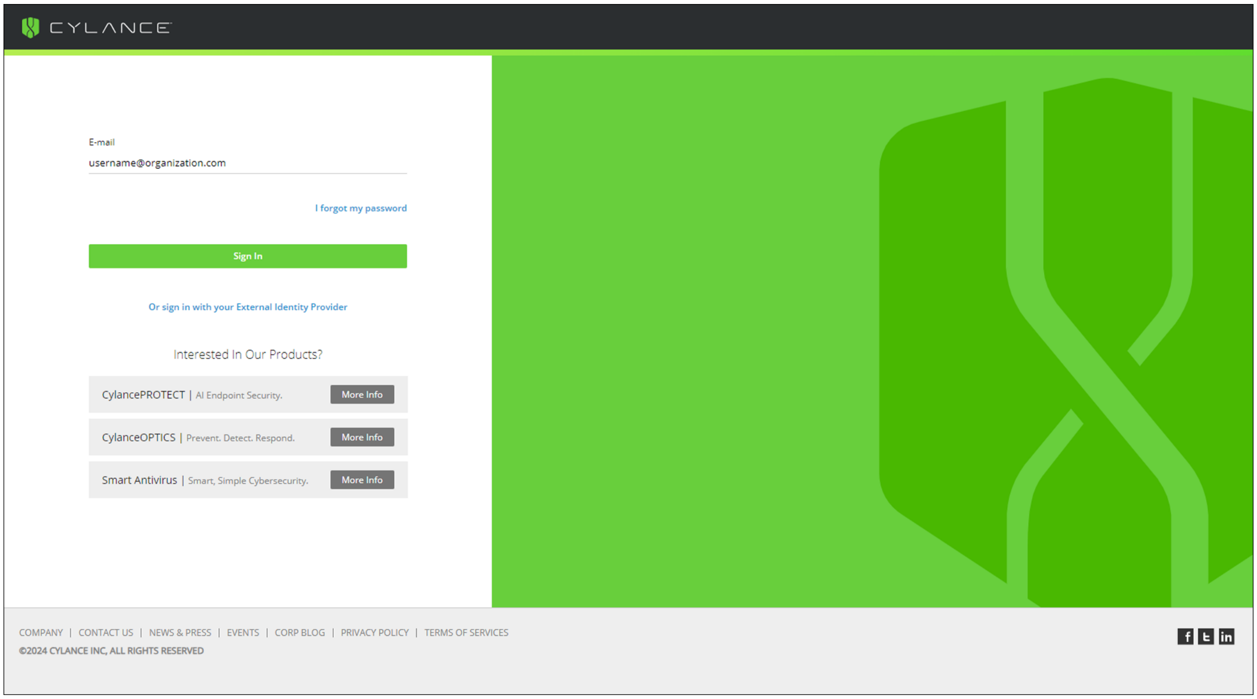
You can expect to receive email messages from CylanceMDR and analysts. To prevent the email messages from being blocked or marked as spam, it is recommended that your email software is configured to allow messages from the certain addresses and domains. The following table lists the email addresses and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

Email address or domain	Description
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.

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 Cylance console to use CylanceMDR



CYLANCE
I forgot my password
Sign In
Or sign in with your External Identity Provider
More Info
More Info
More Info
COMPANY | CONTACT US | NEWS & PRESS | EVENTS | CORP BLOG | PRIVACY POLICY | TERMS OF SERVICES

E-mail
username@organization.com

Interested In Our Products?

CylancePROTECT | AI Endpoint Security.

CylanceOPTICS | Prevent. Detect. Respond.

Smart Antivirus | Smart, Simple Cybersecurity.

©2024 CYLANCE INC, ALL RIGHTS RESERVED

When your organization is subscribed CylanceMDR, the screens and features that are associated with CylanceMDR will be made available in the same Cylance console that is used to manage devices protected by CylancePROTECT, CylanceOPTICS, and CylanceGATEWAY. You must be assigned the Administrator or Read-only roles to have permission to access its features.

The key screens for CylanceMDR in the Cylance console are:

- Dashboard > CylanceMDR Executive Summary
- Dashboard > CylanceMDR Operations
- Dashboard > CylanceMDR Threat Summary
- Alerts > Incidents
- Settings > Escalation Groups

Dashboard

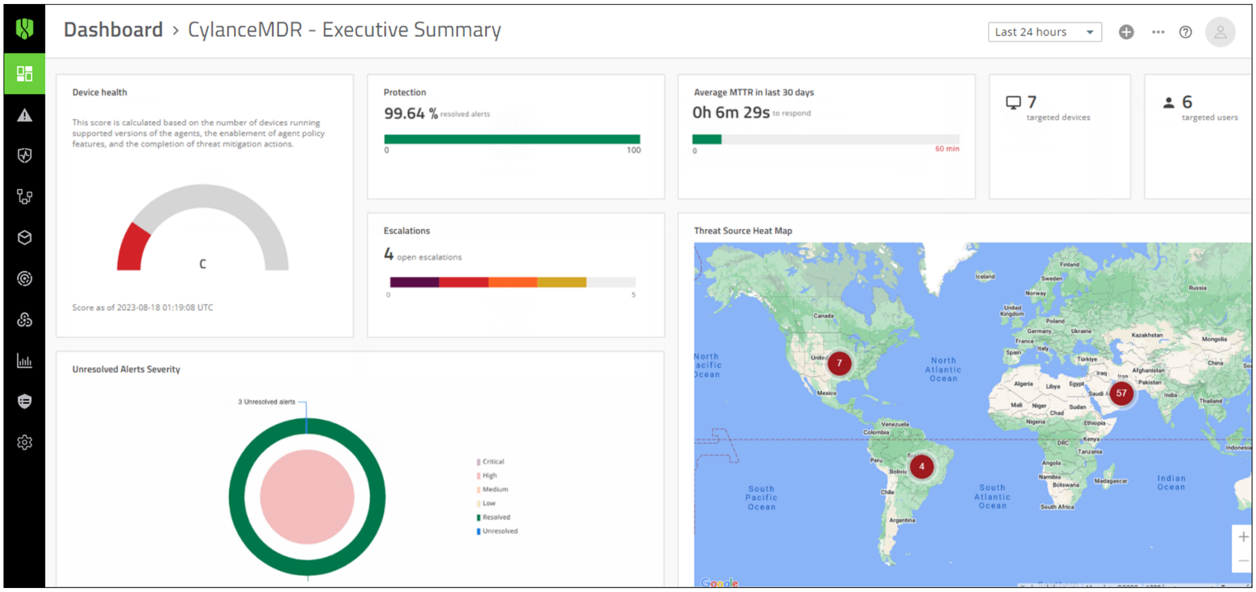
The Dashboard pages for CylanceMDR have an interactive layout that visually displays the various types of alerts that were escalated in your organization, as well as top threats by alert type or target.

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



Dashboard › CylanceMDR - Executive Summary

Last 24 hours

Device health

This score is calculated based on the number of devices running supported versions of the agents, the enablement of agent policy features, and the completion of threat mitigation actions.

Score as of 2023-08-18 01:19:08 UTC

Protection

99.64 % resolved alerts

Average MTTR in last 30 days

0h 6m 29s to respond

7 targeted devices

6 targeted users

Escalations

4 open escalations

Threat Source Heat Map

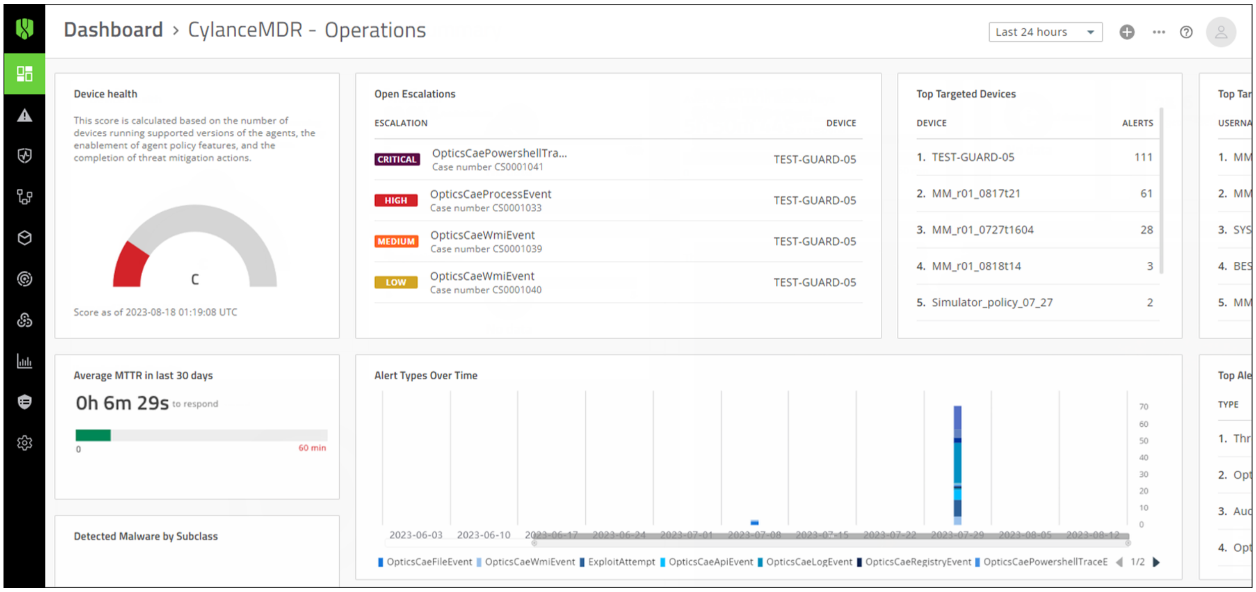
Unresolved Alerts Severity

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



Dashboard › CylanceMDR - Operations

Last 24 hours

Device health

This score is calculated based on the number of devices running supported versions of the agents, the enablement of agent policy features, and the completion of threat mitigation actions.

C

Score as of 2023-08-18 01:19:08 UTC

Open Escalations

ESCALATION		DEVICE
CRITICAL	OpticsCaePowershellTra... Case number CS0001041	TEST-GUARD-05
HIGH	OpticsCaeProcessEvent Case number CS0001033	TEST-GUARD-05
MEDIUM	OpticsCaeWmiEvent Case number CS0001039	TEST-GUARD-05
LOW	OpticsCaeWmiEvent Case number CS0001040	TEST-GUARD-05

Top Targeted Devices

DEVICE	ALERTS
1. TEST-GUARD-05	111
2. MM_r01_0817t21	61
3. MM_r01_0727t1604	28
4. MM_r01_0818t14	3
5. Simulator_policy_07_27	2

Top Tar

USERNA
1. MM
2. MM
3. SYS
4. BES
5. MM

Average MTTR in last 30 days

0h 6m 29s to respond

Alert Types Over Time

Top Ale

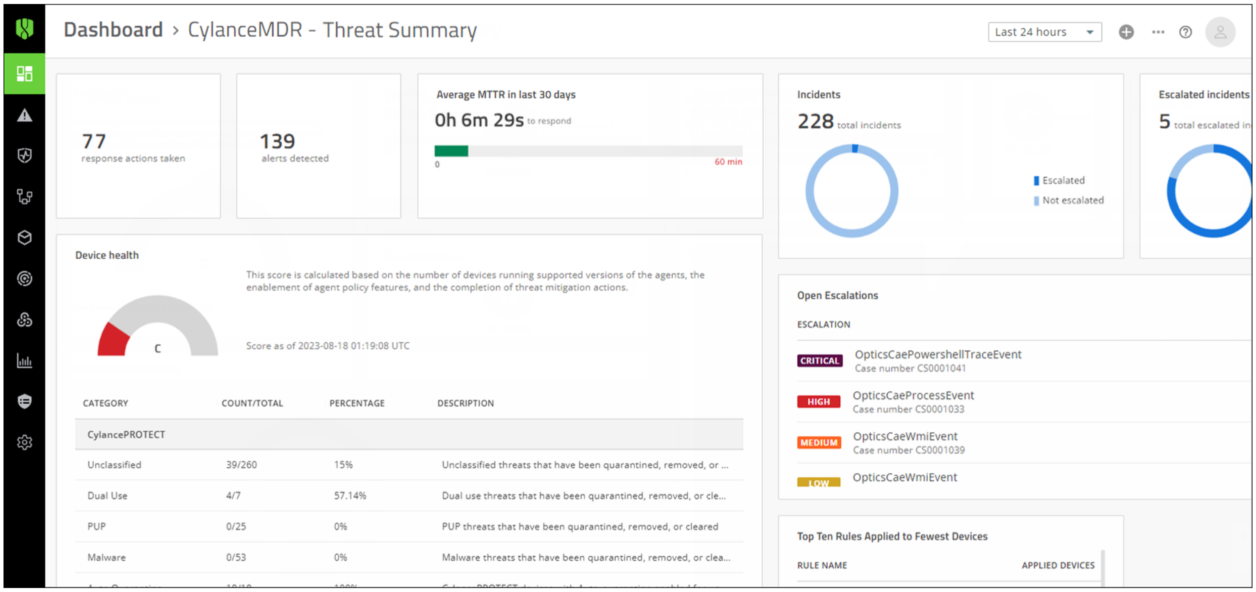
TYPE
1. Thr
2. Opt
3. Auc
4. Opt

Detected Malware by Subclass

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



Dashboard › CylanceMDR - Threat Summary

77
response actions taken

139
alerts detected

Average MTTR in last 30 days
0h 6m 29s to respond

Incidents
228 total incidents

Escalated incidents
5 total escalated in

Device health

This score is calculated based on the number of devices running supported versions of the agents, the enablement of agent policy features, and the completion of threat mitigation actions.

Score as of 2023-08-18 01:19:08 UTC

CATEGORY	COUNT/TOTAL	PERCENTAGE	DESCRIPTION
CylancePROTECT			
Unclassified	39/260	15%	Unclassified threats that have been quarantined, removed, or ...
Dual Use	4/7	57.14%	Dual use threats that have been quarantined, removed, or cle...
PUP	0/25	0%	PUP threats that have been quarantined, removed, or cleared
Malware	0/53	0%	Malware threats that have been quarantined, removed, or clea...

Open Escalations

ESCALATION

CRITICAL	OpticsCaePowershellTraceEvent Case number CS0001041
HIGH	OpticsCaeProcessEvent Case number CS0001033
MEDIUM	OpticsCaeWmiEvent Case number CS0001039
LOW	OpticsCaeWmiEvent

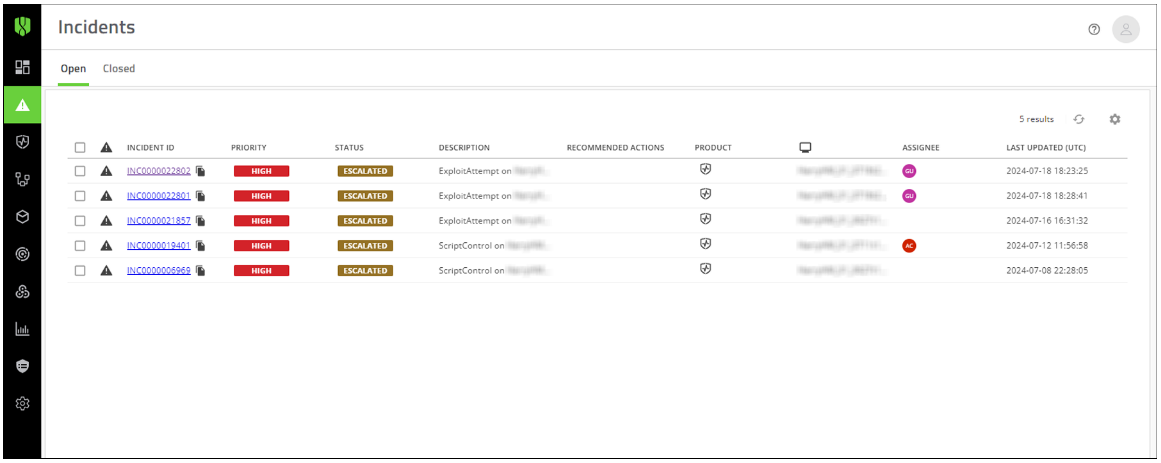
Top Ten Rules Applied to Fewest Devices

RULE NAME	APPLIED DEVICES

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.

Managing incidents



□	⚠	INCIDENT ID	PRIORITY	STATUS	DESCRIPTION	RECOMMENDED ACTIONS	PRODUCT	🖥	ASSIGNEE	LAST UPDATED (UTC)
□	⚠	INC0000022802	HIGH	ESCALATED	ExploitAttempt on [redacted]		⛨	[redacted]	GU	2024-07-18 18:23:25
□	⚠	INC0000022801	HIGH	ESCALATED	ExploitAttempt on [redacted]		⛨	[redacted]	GU	2024-07-18 18:28:41
□	⚠	INC0000021857	HIGH	ESCALATED	ExploitAttempt on [redacted]		⛨	[redacted]		2024-07-16 16:31:32
□	⚠	INC0000019401	HIGH	ESCALATED	ScriptControl on [redacted]		⛨	[redacted]	AC	2024-07-12 11:56:58
□	⚠	INC0000006969	HIGH	ESCALATED	ScriptControl on [redacted]		⛨	[redacted]		2024-07-08 22:28:05

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

If your organization is subscribed to CylanceMDR On-Demand, you must manually request CylanceMDR support from the details screen of an alert from the Alerts page. These requests are escalated to CylanceMDR analysts so they can investigate. You can follow up on these requests from the Alerts > Incidents page in the Cylance console.

On the Incidents page, you can do the following:

- In the Open or Closed tabs, click an incident in the list to view its details.
- Click ⚙ to select the fields that you want to display.
- Export the current list of incidents to a .csv file, or print it as a PDF.

Respond to escalated incidents

When an incident is escalated to your organization, you need to verify its details and determine whether the incident was expected behavior in your environment. You can use the chat feature communicate with a CylanceMDR analyst to share information and take appropriate steps to resolve the incident.

1. In the Cylance console, click **Alerts > Incidents**.
2. Click the **Open** tab.
3. Click an incident.
4. Do any of the following:

Task	Steps
Report whether the incident was expected or unexpected	If you confirm that the incident was based on expected behavior, the incident will be automatically closed. If you report that it was from unexpected behavior, you will be presented additional information and recommended actions to help resolve the threat. **a.** In the dialog message at the top of the screen, click **Expected** or **Unexpected**. **b.** Confirm your selection.
Use the AI-powered Cylance Assistant to investigate alerts in an incident	**a.** Click the **Alerts** tab. **b.** In the **Triggered alert** section, click an alert that triggered the incident. **c.** In the right pane, hover over an instigating process, target process, or script artifact, and click ✦. **d.** At the bottom of the summary in the Cylance AI pane, click ⧉ to copy the analysis.
Assign the incident to an administrator user	**a.** In the left pane, in the **Assignee** field, search for and select another administrator user. **b.** Click **Save**.
Send a message to a CylanceMDR analyst	**a.** In the right pane, click 🗨. **b.** Type your message. **c.** Click **Add**.
Upload attachment to this incident	**a.** In the right pane, click 📎. **b.** Click **Upload**. **c.** Select the file that you want to upload.
View the history of this incident	In the right pane, click 🕓. A history of activity for this incident is displayed.
Close an incident	Send a message to the CylanceMDR analyst (using 🗨) indicating that you want to close the incident. When an incident is closed, it cannot be reopened. You can find closed incidents in the **Closed** tab.

Reports

From the Alert > Incidents page, you can export reports to see more detailed alert metrics for your organization.

You can filter the list of alerts from the Open or Closed tabs based on the information that you're looking for. You can click ⇥ and save the report as a .csv file or print it as a PDF file.

Manage escalation groups

You can add administrator users to escalation groups so that the appropriate administrators are notified based on the severity status of an incident. For example, when the severity of an incident is set to High, members that are in the "-High" escalation group receive a notification.

Only administrator user accounts (such as those that are assigned Administrator or Read-only roles) can be added to an escalation group. For more information about adding administrator users to the Cylance console, see the Cylance Endpoint Security Setup content.

Before you begin: You must be an administrator to manage escalation groups.

1. Click **Settings > Escalation groups**.
2. Click the escalation group that you want to manage.
3. To add a member to the group, click **Add member**.
4. Search for and select the administrators that you want to add.
5. Click **Submit**.