CylanceOPTICS

Migration Guide

Behavioral Detection Engine

Contents

About the Behavioral Detection Engine

The Behavioral Detection Engine (BDE) introduces a new groundbreaking experience for managing CylanceOPTICS detection rules. The BDE simplifies the administration of detection rules and deployments, and includes a set of new detection rules that have been tuned and vetted by our Threat Intelligence team to protect our customers while lessening alert fatigue by limiting alert noise. The BDE also introduces observations, which is the collection of telemetry data for events that occur below the alert threshold configured for your devices.

The BDE has an improved and streamlined process for managing and deploying detection rules. With alert thresholding and observations, the BDE can enact policies with a much lower level of noise without missing important data that may be hiding in low-efficacy signal. The new experience for managing exceptions allows you to define the conditions once, and then assign the exception to devices using flexible assignment criteria such as a global assignment, zones or device policies. This removes the need to duplicate the exception for each policy in your tenant.

This guide highlights some key considerations to help administrators who are already using legacy rulesets transition to use the BDE. You can also review the Behavioral Detection Engine Getting Started Guide, which includes best practices information.

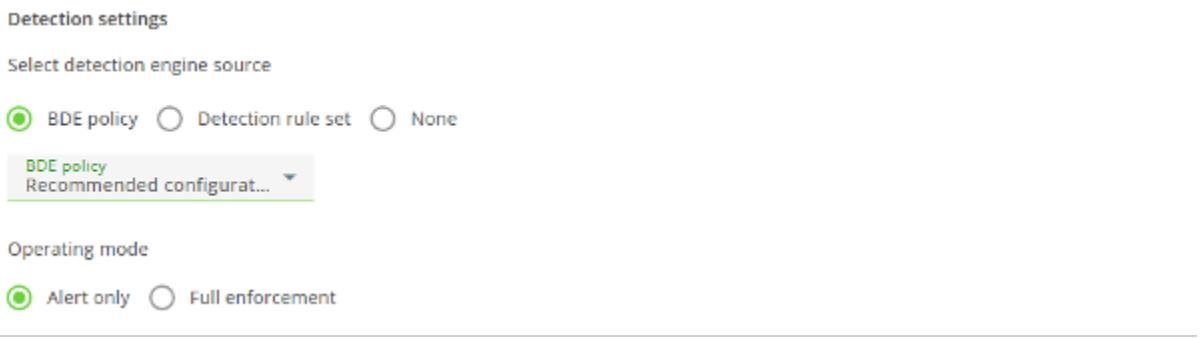
Behavioral Detection Engine features

The is a list of features and improved experiences included with the BDE:

- **Refreshed content library**: A fully redesigned detection rules library that focuses on maximum coverage across MITRE ATT&CK and high-efficacy threat identification.
- **MITRE metadata tagging**: Events are automatically tagged with MITRE tactics and techniques, enabling faster, more targeted threat investigations and richer AI summaries.
- **Observation rules**: The new observation rule type and alert thresholding ensures high-value telemetry is collected without raising unnecessary alerts. This means that the BDE can enact policies with a much lower level of noise without missing important data that may be hiding in a low-efficacy signal.
- **Streamlined exception management**: A new experience for managing exceptions that is decoupled from the policy and centrally managed across the environment for any use case such as tenant, zones, policies, devices.
- **Easier to maintain**: Simplified AI-assisted workflows through the Alerts View makes it easier to tune exceptions with minimal overhead.
- **Automated updates to detection rules**: Delivers frictionless updates to detection rules libraries, reducing operational risks.

Transitioning to the BDE from the legacy ruleset configuration

It is simple to transition devices to BDE policies from legacy rule sets. After you have created a BDE policy, in the device policy that is assigned to the devices, change the **Detection engine source** setting to **BDE policy** and specify the BDE policy to use. This setting removes the legacy detection rules from the device and loads new detection rules provided by the BDE.



These are the suggested migration steps:

1. Create a BDE policy, and then set the operating mode to "Alert only".
2. Create a new test device policy, and then assign a set of devices from across the organization to it for testing purposes. It is important to include devices from users with different roles so that all applications that are used in your organization are tested.
3. In the test device policy, in the **CylanceOPTICS** settings tab, specify the BDE policy in the **Detection settings** section.
4. On the **Alerts** screen, monitor the alerts for detections triggered by the BDE. Using the **Actions** menu, create exceptions for any alerts with **High** severity and those that may impact devices and users. For example, you may need to add some exceptions for some legitimate business applications so that business continuity is not impacted.
5. When the alerts for this group of test devices do not include any legitimate business applications and no further tuning is required, you can move the devices back to the production device policy.
6. In the BDE policy, enable and configure the automated responses for detection techniques according to the requirements of your organization.
7. In the production device policy, specify the BDE policy from the previous step that has the automated responses enabled, and then set the operating mode to **Full enforcement**.
8. If necessary, create other BDE policies and device policies, and then set and assign the device policies to devices within your tenant accordingly.
9. If widespread business continuity issues arise and devices are impacted, you can set the BDE operating mode from device policy of affected devices to **Alert only**. While in this mode, you can add exceptions and tune your environment to mitigate the impact.

For more information, review the best practices in the Behavioral Detection Engine Getting Started Guide.

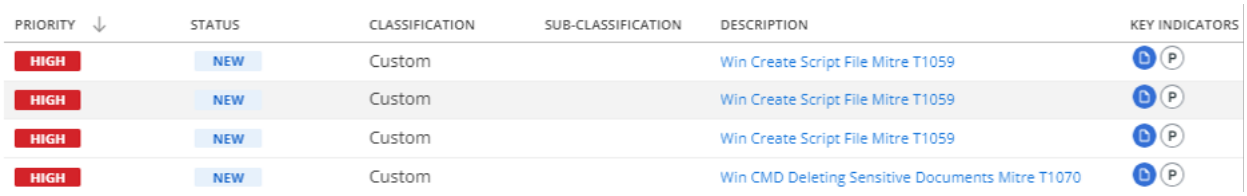
Managing exceptions and tuning your environment

Follow the best practices for tuning your environment that are highlighted in the Behavioral Detection Engine Getting Started Guide. You can create BDE exceptions when viewing alerts from the Alerts screen using AI to automatically define conditions, or you can manually create them from the **CylanceOPTICS > Behavioral Detection Engine > Exceptions** tab.

Viewing BDE detections on the Alerts screen

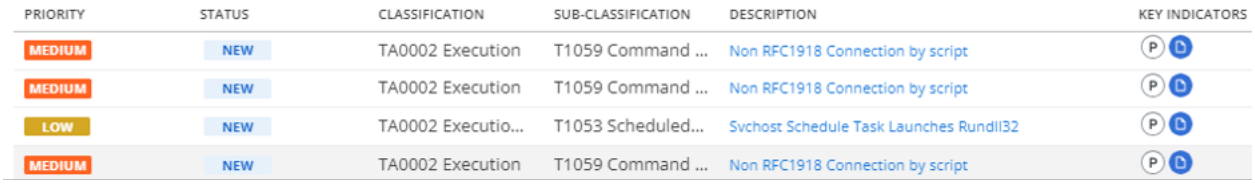
On the **Alerts** screen, detections from the Behavioral Detection Engine (BDE) can be distinguished from detections using the legacy rule sets.

Detections from the legacy rule set have "Custom" or "MitreCA" in the **Classification** column, and the MITRE TTPs in the **Description** column.



PRIORITY	STATUS	CLASSIFICATION	SUB-CLASSIFICATION	DESCRIPTION	KEY INDICATORS
HIGH	NEW	Custom		Win Create Script File Mitre T1059	
HIGH	NEW	Custom		Win Create Script File Mitre T1059	
HIGH	NEW	Custom		Win Create Script File Mitre T1059	
HIGH	NEW	Custom		Win CMD Deleting Sensitive Documents Mitre T1070	

Detections from BDE have the MITRE details in the **Classification** and **Sub-classification** columns.



PRIORITY	STATUS	CLASSIFICATION	SUB-CLASSIFICATION	DESCRIPTION	KEY INDICATORS
MEDIUM	NEW	TA0002 Execution	T1059 Command ...	Non RFC1918 Connection by script	
MEDIUM	NEW	TA0002 Execution	T1059 Command ...	Non RFC1918 Connection by script	
LOW	NEW	TA0002 Executio...	T1053 Scheduled...	Svchost Schedule Task Launches Rundll32	
MEDIUM	NEW	TA0002 Execution	T1059 Command ...	Non RFC1918 Connection by script	

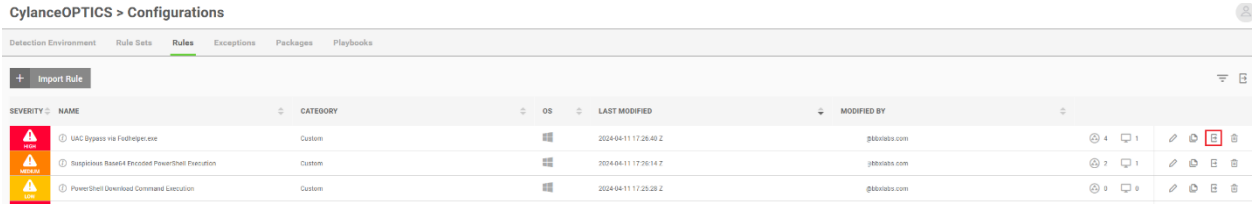
Importing custom rules

The Behavioral Detection Engine supports importing custom detection rules in .json format. In the Cylance console, you can import custom detection rules into custom rule groups from the **CylanceOPTICS > Behavioral Detection Engine > Custom Rules** tab. You can also export legacy rule sets in .json format and import them.

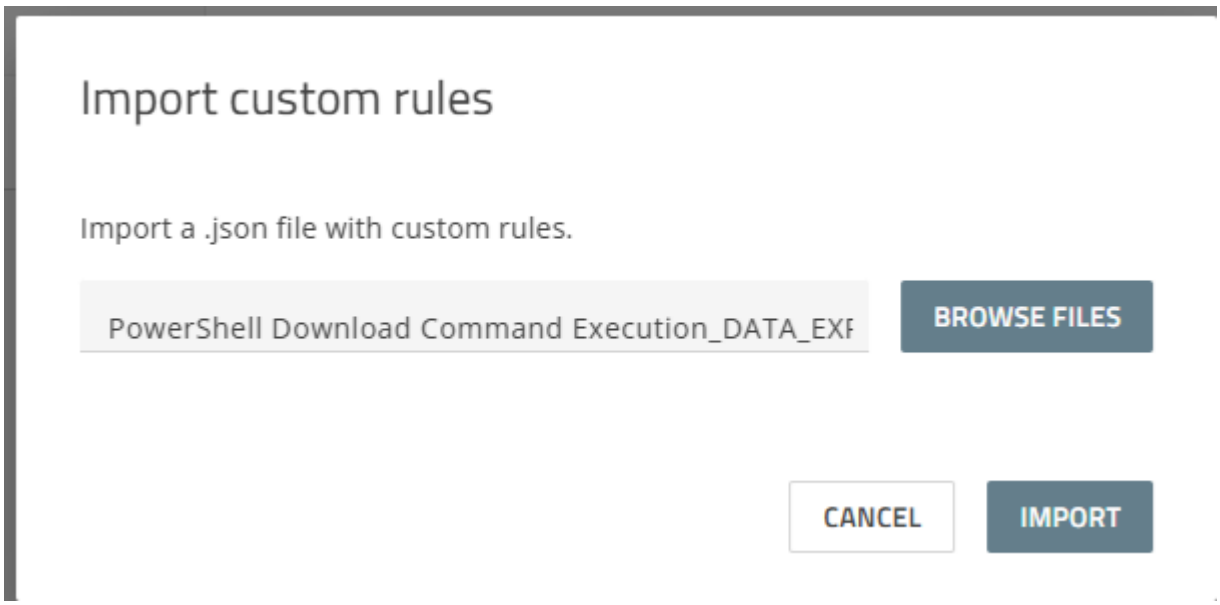
Before you import a custom detection rule, create a custom rule group. The custom rule group that you created appears as a card on the **Custom Rules** screen.

Use these steps to export the legacy rule sets from the Cylance console, create a custom rule group, and then import the legacy rule sets to the custom rule group:

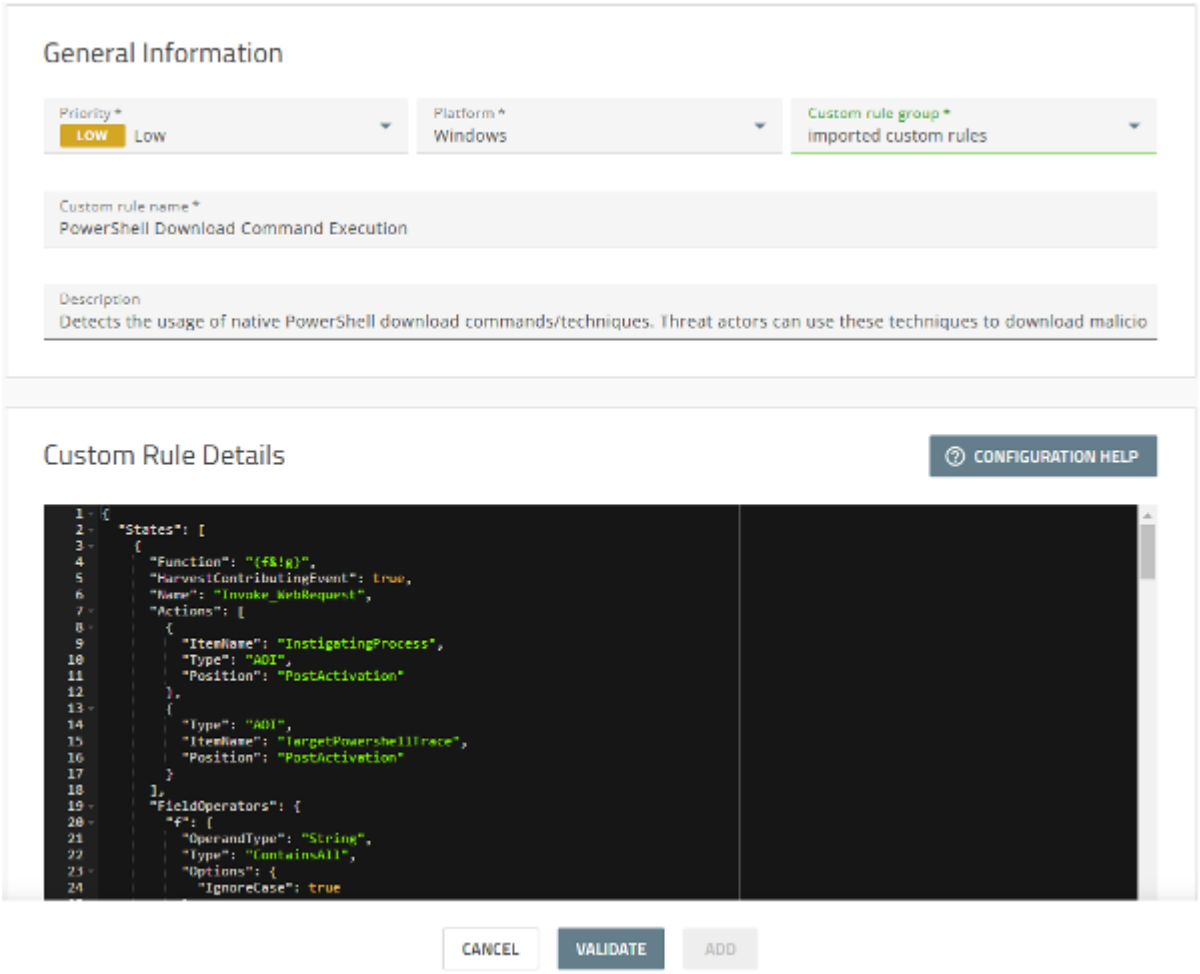
1. Navigate to **CylanceOPTICS > Configurations > Rules**.
2. Beside the rule that you want to export, click **Export** and save the .json file with the rule conditions.



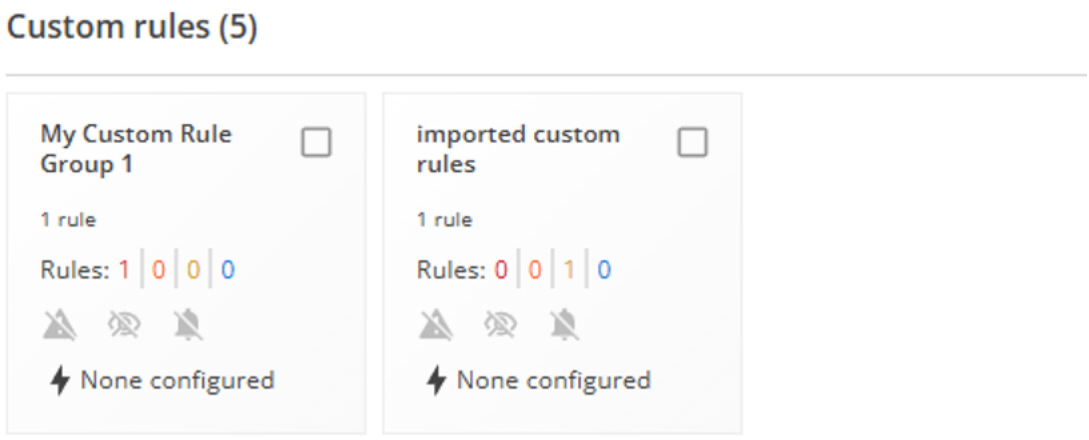
3. Navigate to **CylanceOPTICS > Behavioral Detection Engine > Custom Rules**.
4. In the **Custom Rule** tab, click **Add** and then add a new custom rule group.
5. Click the custom rule group, and then on the right side, click **Add > Import custom rules**, and specify the .json file.



6. Review the imported rule conditions, verify the target custom rule group, and then click **Validate**. After validation, click **Add** to complete the import.



7. On the **Behavioral Detection Engine** screen, **open the BDE policy > Detection And Response** tab where you can enable alerts, observations, and automated responses for your custom rules. The custom rule group will appear as a new card at the bottom of the **Detection And Response** tab when editing a BDE policy, under the **Custom rules** section.



Legal notice

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 .https://www.blackberry.com/us/en/legal/third-party-software

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