CylancePROTECT Application for Splunk

Administration Guide

Contents

What is the CylancePROTECT Application for Splunk?

CylancePROTECT identifies and blocks malware and cyber threats before they can affect a device. BlackBerry uses machine learning techniques to effectively render threats useless while using a minimal amount of system resources. CylancePROTECT Desktop lives in the Cylance console, which is a cloud-based management console that allows you to view various threat-related events, manage device policies to configure agents on endpoints, and manage global lists for quarantined and safe files. For more information about CylancePROTECT, see What is CylancePROTECT Desktop?

The CylancePROTECT Application for Splunk is a plugin within your Splunk environment that pulls data from the Cylance services in your Cylance console to aggregate preconfigured, but customizable, dashboards to monitor, track, and analyze threat data and activity. You can also install the CylancePROTECT Add-on for Splunk Enterprise to further enhance the application's data optimization and collection. This add-on should be installed on Splunk indexers and forwarders that do not consume data from the threat data report.

Requirements: CylancePROTECTApplication for Splunk

Item	Requirements
Splunk	• Splunk version 7.2 or later
Network	• Connections over port 443 must be allowed for the CylancePROTECT Application for Splunk to get threat data reports from Cylance Endpoint Security. • To forward syslog events from Cylance Endpoint Security to your Splunk environment, you must configure network settings in the Cylance console and a log forwarder or firewall rule in your Splunk environment. For more information, see the Cylance syslog guide.

Installing and configuring the CylancePROTECT Application for Splunk

Step	Action
1	Review the CylancePROTECT Application for Splunk requirements.
2	Install the CylancePROTECT Application for Splunk from the Splunk web app manager. If you want to install the CylancePROTECT Application for Splunk manually, see Install the CylancePROTECT Application for Splunk manually.
3	Configure an event index.
4	Configure the syslog data connection.
5	Optionally, if you want to configure the syslog data connection over SSL, see Configuring the syslog data connection over SSL in Splunk.
6	If you want the CylancePROTECT Application for Splunk to receive threat data reports, see Configure threat data reporting.

Install the CylancePROTECT Application for Splunk from the Splunk web app manager

Before you begin: Review the requirements for the CylancePROTECT Application for Splunk.

1. In Splunk, in the horizontal menu bar, click **Splunk>enterprise**.
2. In the vertical **Apps** pane, click **+ Find More Apps**.
3. In the **Browse More Apps** page, search for `CylancePROTECT Application for Splunk`.
4. Click **Install**.
5. Type your Splunk.com username and password.
6. To confirm that you have read the application's terms and conditions, click the check box.
7. Click **Login and Install**.

After you finish: Configure an event index.

Install the CylancePROTECT Application for Splunk manually

Before you begin: Review the CylancePROTECT Application for Splunk requirements.

1. To log in to Splunkbase, navigate to login.splunk.com and type your credentials.

2. On the menu bar, in the search bar, search for `CylancePROTECT App for Splunk`.
3. On the product page, click **Download**.
4. To acknowledge that you have read the terms and conditions, click the check box.
5. Click **Agree to Download**.
6. To manually unpack the .spl ==.tar.gz package, follow the instructions for your OS:

OS package	Steps
Linux package	**a.** Copy the following Splunk package to $SPLUNK_HOME/etc/apps: cylance_protect-<*version*>.spl A cylance_protect folder is created in $SPLUNK_HOME/etc/apps. **b.** Verify that the app files and folders are assigned to the appropriate owner and permissions. $SPLUNK_HOME is located in the /opt/splunk folder.
Windows package	**a.** Copy the following Splunk package to $SPLUNK_HOME\etc\apps: cylance_protect-<*version*>.spl **b.** Unpack the cylance_protect-<*version*>.spl zip folder. A cylance_protect folder is created in $SPLUNK_HOME\etc\apps. $SPLUNK_HOME is located at C:\program files\splunk.

After you finish: Configure an event index.

Configure an event index

The data that Splunk processes resides in an index. Splunk does not create an index by default, so you must set up an event index after you install the CylancePROTECT Application for Splunk. An event index can hold any type of data.

Before you begin:

- Install the CylancePROTECT Application for Splunk from the Splunk web app manager
- If you want to install the CylancePROTECT Application for Splunk manually, see Install the CylancePROTECT Application for Splunk manually.

1. In Splunk, on the menu bar, click **Settings** > **Indexes** > **New Index**.
2. In the **New Index** dialogue box, fill in the fields.

   We recommend you use cylance_protect as the index name. If you use a custom index name, the eventtype=cylance_index must be modified to accept the custom index name.
3. Click **Save**.
4. On the menu bar, click **Settings** > **Event Types** to confirm that the search string appears as `index=protect OR index=Cylance_protect`.
5. In **Settings**, click **Advanced Search** > **Search Macros** and confirm that the search string appears as `index=protect OR index=Cylance_protect`.

   When you upgrade your Splunk environment, there should be an existing index, and the existing configuration files in local should contain the correct file name. In some cases, local files that may have been created for previous installations (for example, files that contain default.xml) will override menus added in

the new release. To correct this, either delete the local file or restart the Splunk search head using the `$SPLUNK_HOME/bin/splunk restart` command.

After you finish: Configure the syslog data connection.

Configure the syslog data connection

The CylancePROTECT Application for Splunk can consume real-time syslog data from the Cylance console. To send these events to Splunk, syslog forwarding needs to be enabled and configured within Splunk and in the Cylance console. For more information about how to configure forwarding, see Configure Splunk indexing and forwarding to use TLS certificates.

Before you begin: Configure an event index.

1. In Splunk, on the Splunk menu bar, click **Settings** > **Data Inputs** > **TCP**.

   For multi-tenant configuration, each tenant will require its own stanza in inputs.conf, and each tenant requires its own port. For example, if there are two tenants, CompanyOne and CompanyTwo, the inputs.conf file should follow the model below:

   ```
   [tcp-ssl://6514]
   disabled = false
   sourcetype = syslog_protect
   source = CompanyOne
   index = cylance_protect
   ```

   ```
   [tcp-ssl://6515]
   disabled = false
   sourcetype = syslog_protect
   source = CompanyTwo
   index = cylance_protect
   ```

2. In the **Port 6515** row, in the **Status** column, click **Enable**.
3. In the Cylance console, on the menu bar, click **Settings** > **Application**.
4. Select the **Syslog/SIEM** check box.
5. Choose the desired event types.
6. In the **SIEM** drop-down list, click **Splunk**.
7. In the **Protocol** drop-down list, click **TCP**.
8. In the **IP/Domain** field, type the IP address or FQDN of your forwarder or Splunk environment.
9. In the **Port** field, type the port number of your Splunk environment.
10. Click **Save**.

After you finish: Optionally, to encrypt the syslog data connection with SSL, see Configuring the syslog data connection over SSL in Splunk.

Configuring the syslog data connection over SSL in Splunk

This section covers the configuration of a syslog data connection over SSL between your Cylance console and Splunk environment. Configuring the connection over SSL encrypts the communication between your Cylance console and Splunk environment, providing an additional layer of security to the data sent by the two systems. You can configure Syslog over SSL in Splunk by generating your own certificates.

Configure the syslog data connection over SSL for Linux Splunk

Before you begin: Configure the syslog data connection.

1. In the Cylance console, click **Settings** > **Application** and select the TLS/SSL box.
2. From the Splunk server command line, using the script below, generate certificates.

```
mkdir /opt/splunk/etc/certs
export OPENSSL_CONF=/opt/splunk/openssl/openssl.cnf
/opt/splunk/bin/genRootCA.sh -d /opt/splunk/etc/certs
/opt/splunk/bin/genSignedServerCert.sh -d /opt/splunk/etc/certs -n splunk -c
splunk -p
```

3. In the $SPLUNK_HOME/etc/apps/cylance_protect/local/inputs.conf file, modify the two sections below using the following attributes:

```
[tcp-ssl://6514]
disabled = false
sourcetype = syslog_protect
index = cylance_protect
source = <YourTenantNameHere>
```

```
[SSL]
serverCert = /opt/splunk/etc/certs/splunk.pem
sslPassword = <The password that was used in the genSignedServerCert command
 above>
requireClientCert = false
```

4. Using the script below, restart Splunk and verify the open port.

```
$SPLUNK_HOME/bin/splunk restart splunkd
netstat -an | grep :6514
```

After you finish: If you want the CylancePROTECT Application for Splunk to receive threat data reports, see Configure threat data reporting.

Configure the syslog data connection over SSL for Windows Splunk

Before you begin: Configure the syslog data connection.

1. In the Cylance console, click **Settings** > **Application** and select the TLS/SSL box.
2. From the Splunk server command line, using the script below, generate certificates.

```
mkdir c:\progra~1\Splunk\etc\certs
C:\progra~1\Splunk\bin\splunk.exe cmd cmd.exe /c c:\progra~1\Splunk\bin
\genRootCA.bat -d c:\progra~1\Splunk\etc\certs
C:\progra~1\Splunk\bin\splunk.exe cmd python c:\progra~1\Splunk\bin
\genSignedServerCert.py -d c:\progra~1\Splunk\etc\certs -n splunk -c splunk -p
```

3. In the C:\Program Files\Splunk\etc\apps\cylance_protect\local\inputs.conf file, modify the two sections below using the following attributes:

```
[tcp-ssl://6514]
disabled = false
sourcetype = <syslog_protect>
index = <cylance_protect>
```

```
source = <YourTenantNameHere>
```

```
[SSL]
sslPassword = <The password that was used in the genSignedServerCert command
 above>
requireClientCert = false
serverCert = c:\progra~1\Splunk\etc\certs\splunk.pem
```

4. Using the script below, restart Splunk and verify the open port.

```
c:\progra~1\Splunk\bin\splunk.exe restart
netstat -an | findstr :6514
```

After you finish: If you want the CylancePROTECT Application for Splunk to receive threat data reports, see Configure threat data reporting

Configure threat data reporting

If you cannot consume syslog data, or if you want to have backward compatibility with previous versions of this application, you can configure threat data reports (TDR) to receive daily report data from Cylance Endpoint Security. The CylancePROTECT Application for Splunkcan process data from the Devices, Events, Indicators, and Threats reports.

Before you begin: Configure the syslog data connection.

1. In the CylancePROTECT Application for Splunk, on the menu bar, click **Help** > **ConfigureTDR**.
2. In the **Add Tenant** section, specify the following:
   - **Tenant Name**: Enter the name of your company.
   - **URL**: Enter the invitation URL.
   - **Token**: Enter the installation token.

   To find the values of the fields, in the Cylance console, click **Settings** > **Application**.
3. Click **Add**.

   If an administrator deletes or regenerate the token, you must update the ConfigureTDR page with the new token.
4. Restart Splunk. After you restart Splunk, you will see the threat data reports in your Splunk environment.

After you finish: In a single-instance Splunk installation or on a heavy forwarder, complete the following steps to enable data inputs:

1. In Splunk, on the Splunk menu bar, click **Settings** > **Data inputs**.
2. In the **Local Inputs** section, click **scripts**.
3. In the **Status** column, click **Enable** for each script.
   To find the values of the fields, in the Cylance console, click **Settings** > **Application**.

Configure adaptive response

The CylancePROTECT Application for Splunk is part of Splunk's adaptive response program. This integration allows you to investigate malicious activities and respond in real-time to cyber threats detected by Cylance Endpoint Security in your organization's Splunk environment. To use adaptive response, you will need to set up an API connector in your Cylance console and Splunk environment.

1. Log in to the Cylance console as an administrator.
2. On the menu bar, click **Settings** > **Integrations**.
3. Click **Add Application**.
4. In the **Application Name** field, type `Splunk API Connector`.
5. In the **Global Lists** row, select the **Read, Write, and Delete** check box.
6. Click **Save**. Record the Application ID, Application Secret, and Tenant ID.
7. In the Splunk server, on your desired Splunk search head, edit the api.py configuration file found in `SPLUNK_HOME/etc/apps/cylance_protect/bin/api.py`.
8. In command lines 9-12, add the Application ID, Application Secret, and Tenant ID that your recorded.
9. In the CylancePROTECT Application for Splunk, click **Tools** > **API Connector**.
10. In the drop-down list, select a function. For a list of the functions and their parameters, refer to the **Usage** chart on the **API Connector** page.
11. In the **Parameter** field, type the file hash.
12. Click **Submit**.
13. Review the HTTP response result at the bottom of the **API Connector** page. To check the HTTP response results from the Cylance console. Refer to the **HTTP Responses** chart for a list of HTTP responses and their meanings.

If API calls fail after editing the api.py configuration file, the *.pyc files may need to be deleted from the `$SPLUNK_HOME/etc/apps/cylance_protect/bin/` directory.

After you finish: You can restrict access to the API connector. If an SOC of IR role exists within your Splunk

1. In Splunk, click **Settings** > **Roles** > **Add New**.
2. In the **Role Name** field, type `CylanceAPI`.
3. Click **Save**.
4. To set permissions for the role, click **Settings** > **All Configurations**.
5. In the **filter** field, search for `api_connector`.
6. In the **Sharing** column, click **Permissions** and confirm the following:
   - For the **Everyone** role, ensure that **Read** and **Write** are deselected.
   - For the **CylanceAPI** role, ensure that **Read** is selected.

Data source types

Syslog events

The syslog-based source types for the CylancePROTECT Application for Splunk provide real time information on threats, devices, threat classifications, memory protection, application control, and audit log.

Source type	Description
Application control	Syslog will report any events detected on devices, including denied attempts to create or modify applications, or to execute files from a network or external location.
Audit log	Syslog will report all user actions performed on the Cylance console by administrators, zone managers, and users.
Devices	Syslog will report devices that have been registered, modified, or removed.
Device control	Syslog will report device control events like the device type, vendor ID, and product ID.
Memory protection	Syslog will report any malicious processes and exploits that were detected and/or blocked by this script.
Script control	Syslog will report all scripts that ran or attempted to run.
Threats	Syslog will report any newly found threats in your environment as well as any changes observed for existing threats.
Threat classifications	Syslog will report any newly classified threats or changes to existing threat classifications.

Threat data report

The threat data report-based source types for the CylancePROTECT Application for Splunk are extracted from the CylancePROTECT threat data report, which list the threats and devices in your environments.

Script	Description
Threats	The Threats script reports all threats that are detected in your environment, along with relevant information such as file name, file hashes, file status, and Cylance Score.
Devices	The Devices script reports all CylancePROTECT Desktop registered devices in your organization, along with information such as each device's operating system, agent version, and MAC address.
Indicators	The indicators script reports each threat with a unique SHA256 hash and all associated threat indicators that characterize the file. For more information about threat indicators, see KB 66181.

Script	Description
Events	The Events script will report all threat events that occurred in your organization for the last 30 days. This information includes the file hash, the device name, the file path, the date and time it was found, the threat status, and the Cylance Score.

Troubleshooting the CylancePROTECT Application for Splunk

This section details issues that you may encounter with the CylancePROTECT Application for Splunk and the actions that you can take to resolve them.

Customize how the CylancePROTECT Application for Splunk generates log files

If an issue arises, such as when the post-install test doesn't result in observable output, you will need to examine splunkd.log and Cylance.log files in the $SPLUNK_HOME/var/ logs/ Splunk directory.

To generate detailed log data, do the following:

1. In the config.py file, in the bin directory, change the log level to one of the following:
   - DEBUG
   - INFO
   - WARNING
   - ERROR
   - CRITICAL
   - FATAL
2. In the config.py file, change any of the following parameters to customize log file generation:
   - **Filename**: The default file name is cylance.log.
   - **Size**: The default maximum log size is 1,000,000 bytes. When the files exceeds this size, a new log file is created.
   - **Rotations**: This is the number of log files that can be created before the oldest is overwritten.

Troubleshoot syslog consumption

If data does not populate in the syslog dashboard, do the following:

- If your organization uses a distributed Splunk environment, verify that syslog consumption is configured on the forwarder and that the Splunk environment is running on version 7.2 or later.
- Verify that the latest version of the CylancePROTECT Application for Splunk is installed on the Splunk search head and that the matching version of the technology add-on is installed on indexers and forwarders.
- Verify that the index name is either `cylance_protect` or `protect` to match the inputs.conf file.
- Verify that the incoming source type define in inputs.conf is `syslog_protect`.
- Confirm that the eventtype.conf file, which populates the dashboards, has not been altered.
- Verify that the macro `cylance_index`, which searches for Cylance data, has not been altered.
- On the Splunk homepage, in the vertical menu bar, click **Search & Reporting**. Set the time preset to **All Time (real-time)**, then run the`eventtype=cylance_index sourcetype=syslog*` command.

Outcome	Actions to resolve
No data is returned.	• Click **Test Connection** in the Cylance console. You should see a **Test Connection Successful** message. • Verify that the port is open to receive syslog data. For example, for port 651, you should use the `netstat – an |grep 6514` command. • Confirm that no network or host firewalls are blocking traffic. You may need to configure layer 7 firewalls to receive TLS/SSL traffic. • Use a packet sniffer to verify that syslog is successfully connected and that data is passing through your networks. • If the Splunk environment uses a syslog daemon to write the data to a file first, ensure that the data is being written to the file as expected.
Data is returned but is illegible.	Verify that the TLS configuration is consistent in the Cylance console and in Splunk. For example, the TLS/SSL check box is selected in the Cylance console and tcp-ssl is used in the Splunk inputs.conf file.
Data is only returned from the syslog_protect source type.	Verify that the app is installed on the forwarder and search head so that the props.conf and transforms.conf take effect and properly rename `sourcetype=syslog_protect` to another source type name, based on the content of the event.

Troubleshoot threat data reporting

If data does not populate in the report dashboard, do the following:

- If your organization uses a distributed Splunk environment, verify that threat data report consumption is configured on a heavy forwarder that is running the CylancePROTECT Application for Splunk (not just the technology add-on) and that the Splunk environment is running on version 7.2 or later.
- Verify that the latest version of the application is installed on the Splunk search head and that the matching version of the technology add-on is installed on the indexers.
- Confirm that the index name is either `cylance_protect` or `protect` to match the inputs.conf file.
- Confirm that the eventtypes.conf file, which populates the dashboards, has not been altered.
- Verify that the macro `cylance_index`, which searches for Cylance data, has not been altered.
- On the Splunk homepage, on the vertical menu bar, click **Search & Reporting**. Set the time preset to **All Time (real-time)**, then search for the`eventtype=cylance_index sourcetype=syslog*` command.

  From the command line, check the cylance_protect/local directory for the presence of CSV and SHA files (for example, <*TenantName*>-`event.csv` or <*TenantName*>-*`indicators.sha`*).

Outcome	Actions to resolve
The CSV and SHA files are present.	• Check the $SPLUNK_HOME/etc/apps/cylance_protect/defaults/ inputs.conf file for the index name that the scripted inputs are using. • Verify that the index exists. Use the index name to search on the Splunk search bar.

Outcome	Actions to resolve
The CSV and SHA files are not present.	• Verify that your Splunk environment is not behind a proxy or firewall that could be blocking the connection. If a proxy or firewall is blocking the connection, configure it to allow connections to the Cylance console. • Run the cy_test.py script from the command line.

Remove the CylancePROTECT Application Splunk

1. Do any of the following:

Task	Steps
Linux: Remove the application and leave the associated data intact.	Run the following command: `./splunk remove app [appname]`

Linux: Remove the application and associated data.	**a.** To remove the data, run the following command:
	`./splunk remove index <Your Index Name>`
	b. To remove the application, run the following command:
	`./splunk remove app [appname].`

Windows: Remove the application and leave the associated data intact.	Run the following command: `splunk remove app [appname]`

Windows: Remove the application and associated data.	**a.** To remove the data, run the following command:
	`./splunk remove index <Your Index Name>`
	b. To remove the app, run the following command:
	`splunk remove app [appname]`

Deactivate the CylancePROTECT Application for Splunk.	Run the following command: `./splunk disable app [Cylance_protect] -auth<username>:<password>`
Re-activate the CylancePROTECT Application Splunk. .	Run the following command: `./splunk enable app [Cylance_protect] -auth<username>:<password>`

2. Restart Splunk.

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 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