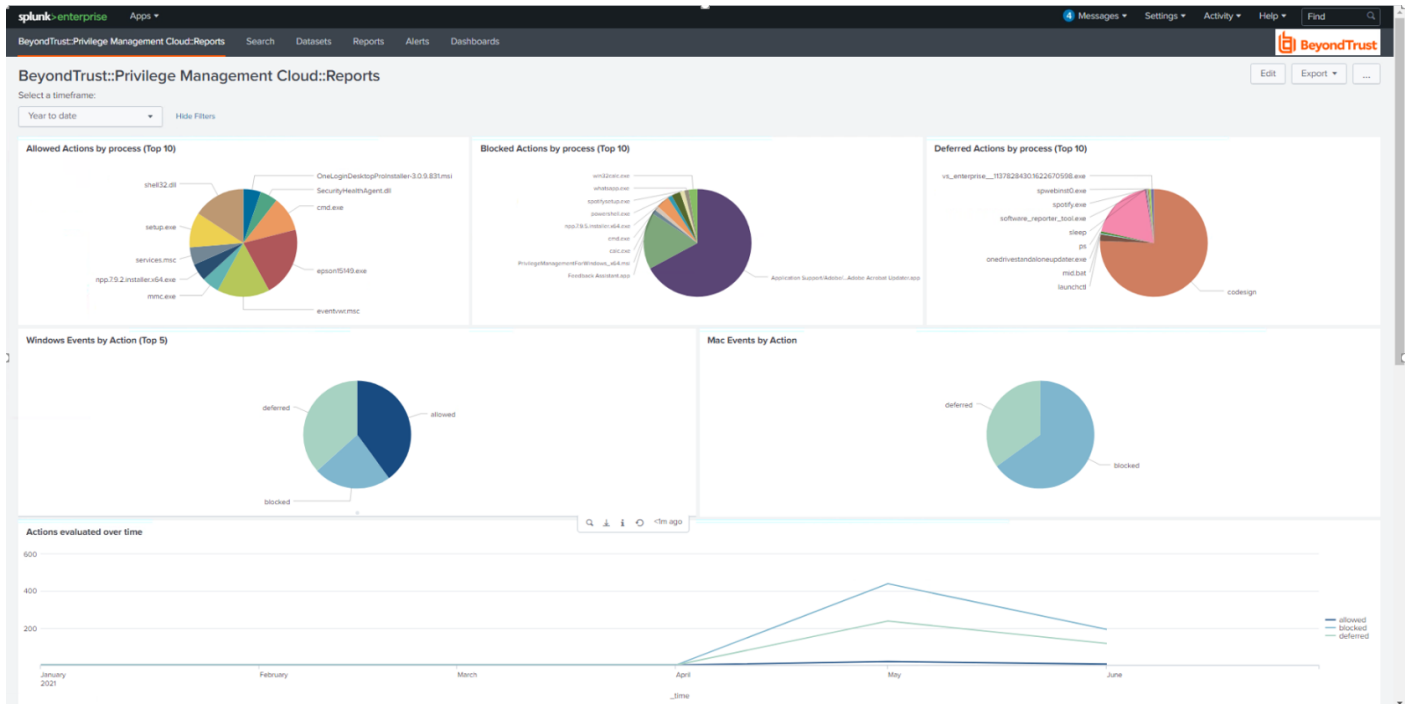


# Use the Splunkbase App for Privilege Management Cloud

The Splunkbase app for BeyondTrust's Privilege Management Cloud allows you to visualize and interpret the large number of events forwarded to Splunk by Privilege Management Cloud. The app consists of a sample of relevant reports in various formats, grouped on a single dashboard.

The dashboard allows you to more rapidly benefit from the integration between PM Cloud and Splunk by leveraging working reports that can be used as is or as templates for custom reports.



## Prerequisites

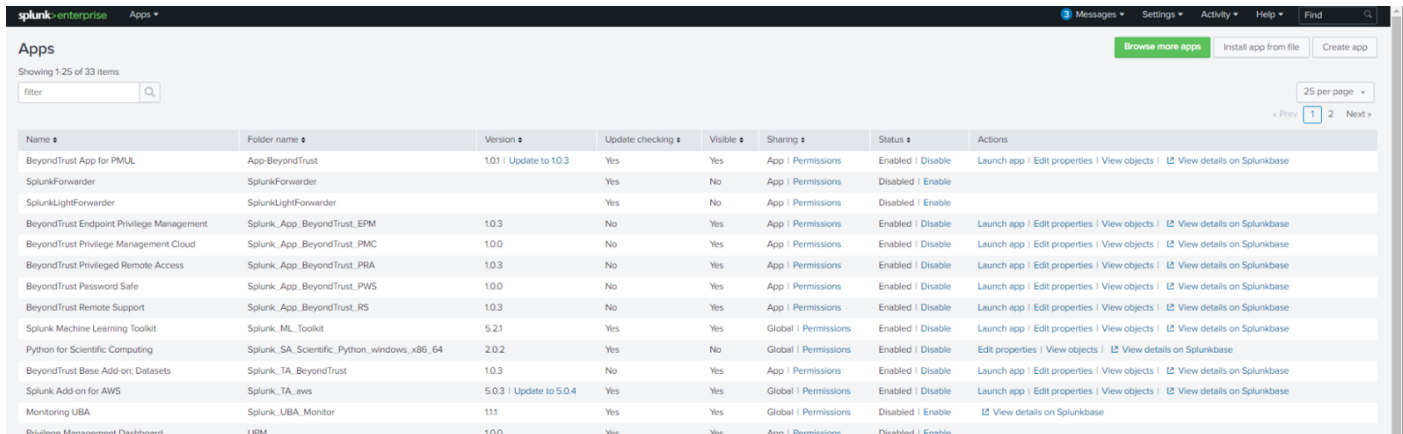
Set up the SIEM settings for Splunk in Privilege Management Cloud. Alternatively, AWS S3 bucket can be used.

**i** For more information on SIEM settings, please see [Configure SIEM Settings](https://www.beyondtrust.com/docs/privilege-management/console/pm-cloud/configuration/configure-siem-settings.htm) at <https://www.beyondtrust.com/docs/privilege-management/console/pm-cloud/configuration/configure-siem-settings.htm>.

## Import the App

Import the app either from Splunkbase or a file. Notifications are received when updates are available (version 1.0 and later).

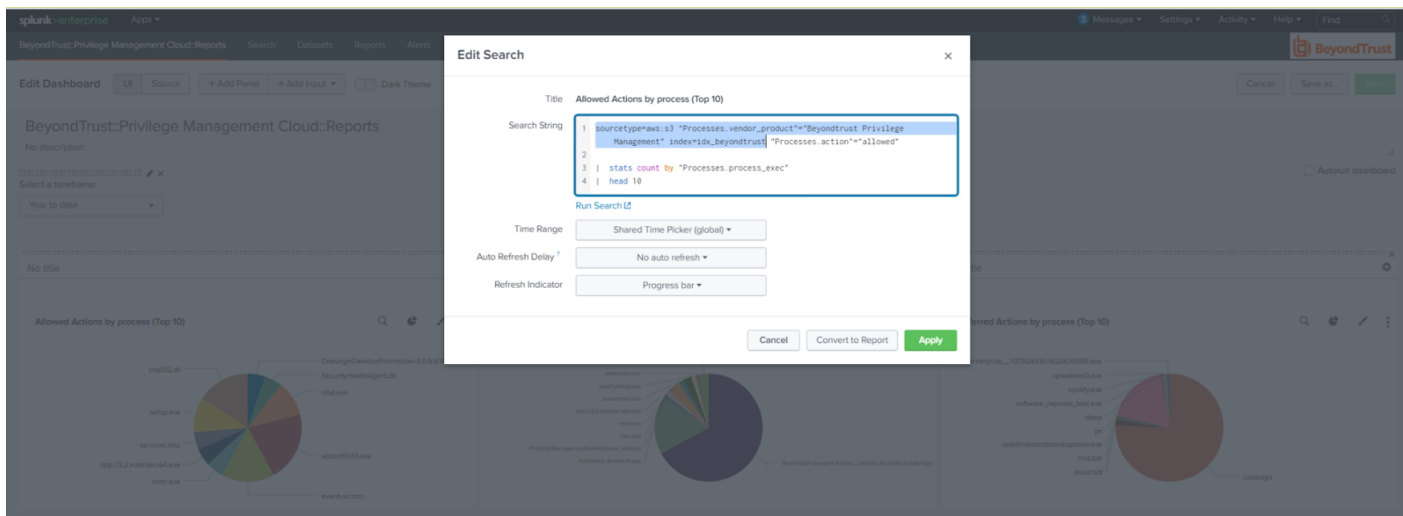
Click **Apps > Manage Apps** to browse Splunkbase and search for the PM Cloud app.



Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
BeyondTrust App for PMUL	App_BeyondTrust	1.01   Update to 10.3	Yes	Yes	App   Permissions	Enabled   Disable	Launch app   Edit properties   View objects   View details on Splunkbase
SplunkForwarder	SplunkForwarder		Yes	No	App   Permissions	Disabled   Enable	
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App   Permissions	Disabled   Enable	
BeyondTrust Endpoint Privilege Management	Splunk_App_BeyondTrust_EPM	10.3	No	Yes	App   Permissions	Enabled   Disable	Launch app   Edit properties   View objects   View details on Splunkbase
BeyondTrust Privilege Management Cloud	Splunk_App_BeyondTrust_PMC	1.0.0	No	Yes	App   Permissions	Enabled   Disable	Launch app   Edit properties   View objects   View details on Splunkbase
BeyondTrust Privileged Remote Access	Splunk_App_BeyondTrust_PRA	10.3	No	Yes	App   Permissions	Enabled   Disable	Launch app   Edit properties   View objects   View details on Splunkbase
BeyondTrust Password Safe	Splunk_App_BeyondTrust_PWS	1.0.0	No	Yes	App   Permissions	Enabled   Disable	Launch app   Edit properties   View objects   View details on Splunkbase
BeyondTrust Remote Support	Splunk_App_BeyondTrust_RS	10.3	No	Yes	App   Permissions	Enabled   Disable	Launch app   Edit properties   View objects   View details on Splunkbase
Splunk Machine Learning Toolkit	Splunk_ML_Toolkit	5.2.1	Yes	Yes	Global   Permissions	Enabled   Disable	Launch app   Edit properties   View objects   View details on Splunkbase
Python for Scientific Computing	Splunk_SA_Scientific_Python_windows_x86_64	2.0.2	Yes	No	Global   Permissions	Enabled   Disable	Edit properties   View objects   View details on Splunkbase
BeyondTrust Base Add-on: Datasets	Splunk_TA_BeyondTrust	10.3	No	Yes	App   Permissions	Enabled   Disable	Launch app   Edit properties   View objects   View details on Splunkbase
Splunk Add-on for AWS	Splunk_TA_aws	5.0.3   Update to 5.0.4	Yes	Yes	Global   Permissions	Enabled   Disable	Launch app   Edit properties   View objects   View details on Splunkbase
Monitoring UBA	Splunk_UBA_Monitor	111	Yes	Yes	Global   Permissions	Disabled   Enable	View details on Splunkbase
Privilege Management Dashboard	LPM	1.0.0	Yes	Yes	App   Permissions	Disabled   Enable	

## Troubleshoot

If reports don't show any data, this might mean there is a mismatch with **source** or **sourcetype** and **index**. If data inputs or the event forwarder cannot be configured for the values expected by the reports and associated queries, an alternative is to edit each report query to resolve mismatches. Each report query can also be tested with Splunk Search app.



**Edit Search**

Title: Allowed Actions by process (Top 10)

Search String:

```

1 | sourcetype=aws:s3 "Processes.vendor_product!="BeyondTrust.Privilege
2 | Management" index="beyondtrust" "Processes.action=="allowed"
3 | stats count by "Processes.process_exec"
4 | head 10
    
```

Run Search

Time Range: Shared Time Picker (global)

Auto Refresh Delay: No auto refresh

Refresh Indicator: Progress bar

Buttons: Cancel, Convert to Report, Apply