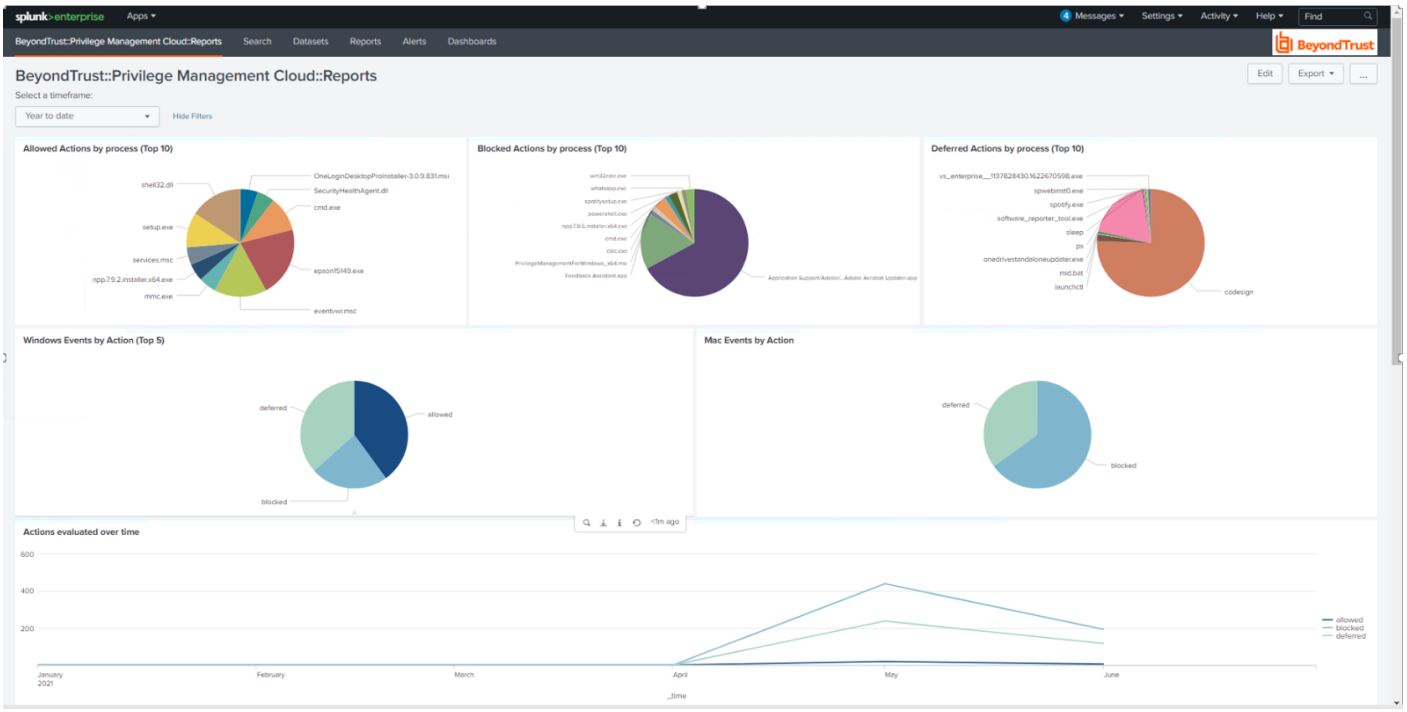
Use the Splunkbase App for Privilege Management Cloud

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

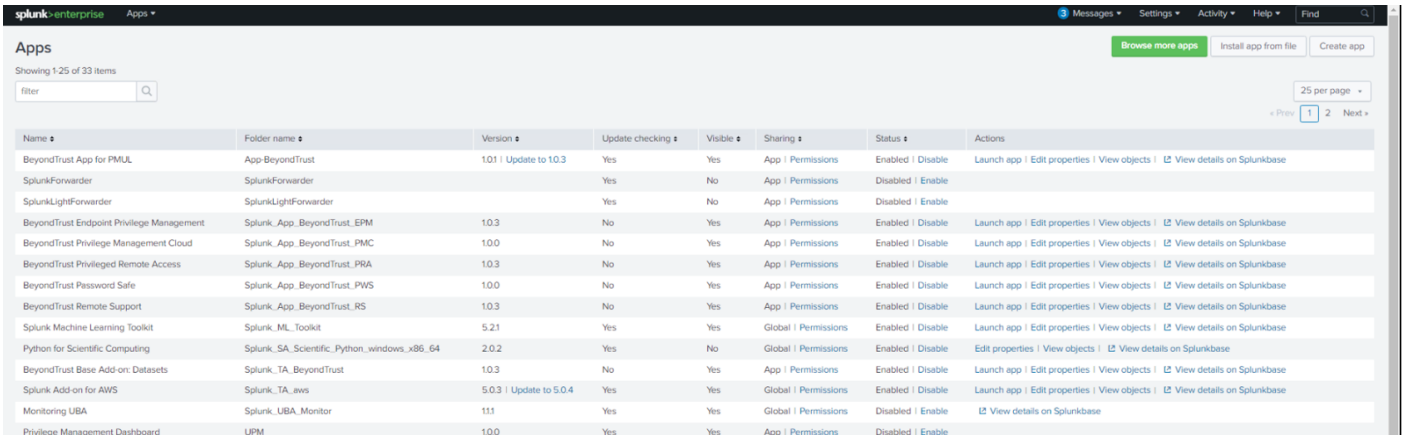
Set up the SIEM settings for Splunk in Privilege Management Cloud. Alternatively, AWS S3 bucket can be used.

> *For more information on SIEM settings, please see Configure SIEM Settings 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.



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.