BeyondTrust

Privileged Remote Access
Splunk Integration

TC:2/8/2019

Table of Contents

BeyondTrust Privileged Remote Access Integration with Splunk

IMPORTANT!

You must purchase this integration separately from both your BeyondTrust software and your Splunk solution. For more information, contact BeyondTrust sales.

IT administrators using Splunk can now integrate BeyondTrust Privileged Remote Access (PRA) to strengthen access control, identify and prioritize threats seamlessly in real time, and remediate incidents proactively.

The BeyondTrust PRA integration helps safeguard your business by giving you complete visibility into activity across the IT infrastructure, including external threats such as malware hackers, internal threats such as data breaches and fraud, risks from application flaws and configuration changes, and compliance pressures from failed audits.

Through the integration, session event data captured through BeyondTrust PRA's rich logging capability is populated into Splunk's platform and reports are provided for security review.

Prerequisites for the BeyondTrust Privileged Remote Access Integration with Splunk

Applicable Versions

- BeyondTrust Privileged Remote Access: 15.x and newer
- Splunk on-premise: 6.3.0 and newer

Network Considerations

The following network communication channels must be open for the integration to work properly:

Outbound From	Inbound To	TCP Port #	Purpose
BeyondTrust Middleware Engine Server	Splunk Server	1514	Session event data is pushed as specially formatted syslog messages into Splunk
BeyondTrust Appliance	Splunk Server	514	Syslog event information from the appliance

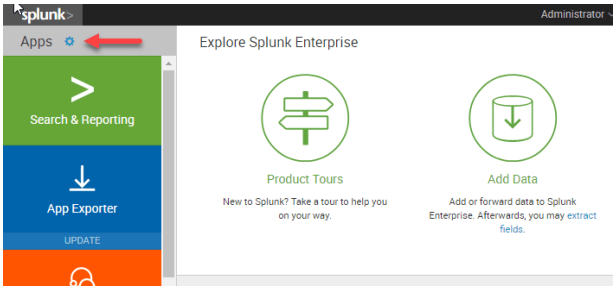
Prerequisite Installation and Configuration

The Splunk integration is a BeyondTrust Middleware Engine plugin. To install the BeyondTrust Middleware Engine, follow the instructions in the BeyondTrust Middleware Engine Configuration document at www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/middleware-engine.

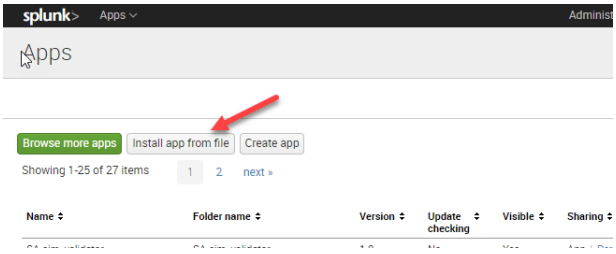
Configure Splunk for Integration with BeyondTrust Privileged Remote Access

To install the integration, follow the steps below to import an item into Splunk.

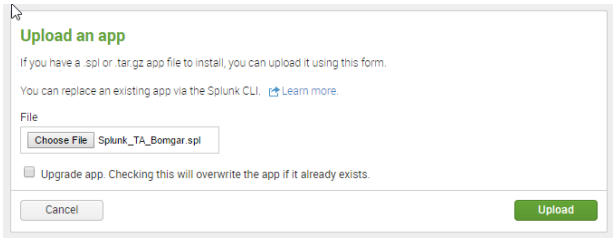
1. Log into Splunk as a user with administrative rights.
2. From the main home page, **/app/launcher/home**, click on the gear icon in the upper-left corner and go to **Manage Apps**.



3. On the **Apps** page, click **Install app from file**.



4. Browse to the location of the **Splunk_TA_BeyondTrustPAM.spl** file and install the **Splunk Technology Add-on**.



Other Considerations

For manual installation not completed through the web user interface, you must determine your deployment method, standalone or distributed. If distributed, your BeyondTrust technical account manager must go to the **Splunk Indexer** or **Forwarder**.

Configure BeyondTrust Privileged Remote Access for Integration with Splunk

In addition to the steps outlined in the BeyondTrust SIEM Tool Plugin Installation and Administration at www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/siem-tool/index, the Splunk integration also supports consumption of syslog output directly from the BeyondTrust Appliance.

All of the steps in this section take place in the BeyondTrust **/appliance** administrative interface.

1. Access your BeyondTrust interface by going to the hostname of your BeyondTrust Appliance followed by /appliance (e.g., **https://access.example.com/appliance**).
2. Go to **/appliance >Security > Appliance Administration** and locate the **Syslog** section.
3. Enter the hostname or IP address for your remote syslog server.
4. Select a message format.
5. Click **Submit**.

Configure the SIEM Tool Plugin for Integration between Splunk and BeyondTrust Privileged Remote Access

In addition to the steps outlined in the BeyondTrust SIEM Tool Plugin Installation and Administration at www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/plugin/index, the Splunk integration also supports consumption of syslog output directly from the BeyondTrust Appliance.

All of the steps in this section take place in the BeyondTrust **/appliance** administrative interface.

Splunk Instance

1. **Target SIEM System:** Select Splunk from the list.
2. **SIEM Syslog Host:** Enter the hostname or IP address of the Splunk instance that should receive messages.
3. **SIEM Syslog Port:** Enter the port used by the Splunk instance to receive syslog messages, usually port 1514.
4. **SIEM Syslog Protocol:** Select the appropriate protocol from the list, usually UDP.
5. **Events to Process:** BeyondTrust session data may contain many different event types. All types are available; however, only a subset may be desired in the SIEM tool. Select only the events you would like sent to Splunk. Events matching unchecked event types are ignored.