BOMGAR™

Splunk
with Bomgar Privileged Access

TC:1/30/2018

Table of Contents

Bomgar Privileged Access Integration with Splunk

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

The Bomgar PA 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 Bomgar PA's rich logging capability is populated into Splunk's platform and reports are provided for security review.

Prerequisites for the Bomgar Privileged Access Integration with Splunk

Applicable Versions

- Bomgar Privileged 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
Bomgar Middleware Engine Server	Splunk Server	1514	Session event data is pushed as specially formatted syslog messages into Splunk
Bomgar Appliance	Splunk Server	514	Syslog event information from the appliance

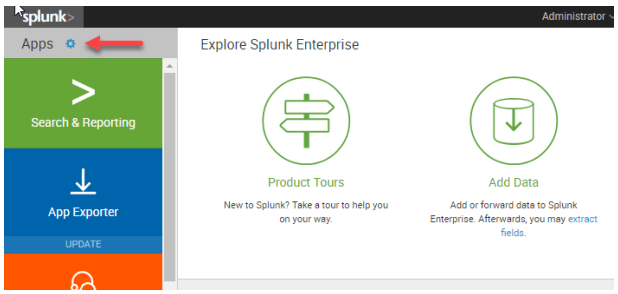
Prerequisite Installation and Configuration

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

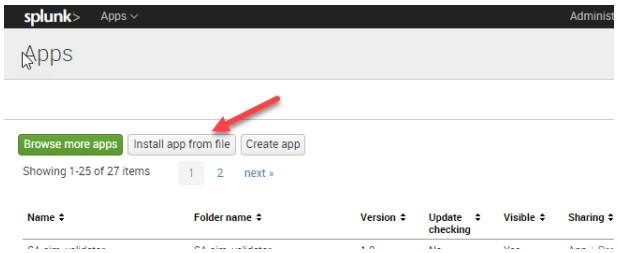
Configure Splunk for Integration with Bomgar Privileged Access

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

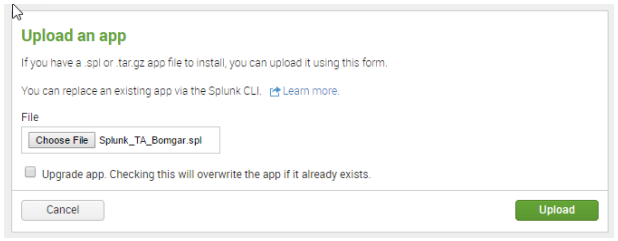
1. Log into Splunk as a user with administrative rights.
2. From the main home page, **/app/launcher/home**, click on the gear icon in the upper-left corner and go to **Manage Apps**.



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



4. Browse to the location of the **Splunk_TA_BomgarPAM.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 Bomgar technical account manager must go to the **Splunk Indexer** or **Forwarder**.

Configure Bomgar Privileged Access for Integration with Splunk

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

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

1. Access your Bomgar interface by going to the hostname of your Bomgar 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 Bomgar Privileged Access

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

All of the steps in this section take place in the Bomgar **/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:** Bomgar 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.