

# BOT RISK SCANNER Integration Guide (VERSION – 1.0.4)





(~

# CONTENTS

Introduction	2
Integration Guidelines	3
1. Download Bot Risk Scanner App from Splunk Marketplace	3
2. Result Index Creation	4
3. Bot Risk Scanner Configuration	5
Post-Install Recommendations.	6
Dashboard & KPI Details	8



### INTRODUCTION

The Radware Bot Risk Scanner (BRS) is a free, Splunk-based bot analyzer that provides comprehensive insights into an application's bad bot traffic without requiring any additional integrations. The tool is available for installation as a plugin on the Splunk Marketplace (Link) and can be easily enabled through the GUI. This plugin offers a detailed dashboard with insights into the application's traffic and the types of bots attempting to access the system. This document outlines the installation process for the Bot Risk Scanner through the Splunk Marketplace.



# INTEGRATION GUIDELINES

To Enable Bot Risk Scanner, follow these 3 simple steps:

#### 1. Download Bot Risk Scanner App from Splunk Marketplace



Login to your Splunk Enterprise/Splunk Cloud account and navigate to the launcher page.

Click on "Find More Apps" to access the App marketplace page.



- In the App Marketplace page search for "Radware Bot Risk Scanner" and install through the link provided.
- Post-installation, navigate to your apps and open the "Radware Bot Risk Scanner"

**Note:** To use the Bot Risk Scanner, you need a Splunk Enterprise or Splunk Cloud account. If you encounter any errors, please refer to the FAQ section for troubleshooting information.



#### 2. Result Index Creation

Once the Radware Bot Risk Scanner is installed, and before configuring it, you need to create a result index in Splunk Enterprise/Cloud to store all the information processed by the Bot Risk Scanner End Point. Follow the steps below to create a new index.

Administrator -	3 Messages ▼ Settings ▼ KNOWLEDGE	Activity ▼ Help ▼ Find DATA	Я	In the Splunk UI, navigate to <b>Settings &gt; Data &gt; Indexes.</b>
Add Data	Searches, reports, and alerts Data models Event types Tags Fields	Data inputs Forwarding and receiving Indexes Report acceleration summaries Virtual indexes	ת	Click on " <b>New Index</b> " to store the information retrieved from Bot Risk Scanner Endpoint.
ŶŶŶ	Lookups User interface	Source types		
New Index General Settings		×	7	Name the New Index as "radware brs result" and select
Index Name	radware_brs_result	ndex=INDEX_NAME.		the app name as " <b>Radware Bot</b> Risk Scanner"
Index Data Type	Events The type of data to store (event-based or metrics).			

**Note:** Users of the Splunk Enterprise version, need to select the app as "**Radware Bot Risk Scanner**" while creating the result index. This is not required for Splunk Cloud version users.

Data Integrity Check	Enable	[	Disable			
	Enable this if you want Splunk to compute hashes on e	very slice of your data fo	or the purpose of data integrity.			
Max Size of Entire Index	500		GB ▼			
	Maximum target size of entire index.					
Max Size of	auto		GB ▼			
Hot/Warm/Cold Bucket	me' for high-volume inde	exes.				
Frozen Path optional						
	Frozen bucket archive path. Set this if you want Splunk	to automatically archive	frozen buckets.			
Арр	Radware Bot	Risk Scanner 🔻				



#### 3. Bot Risk Scanner Configuration

Source Index Name: *	Source Index name to fetch events
Source Field Names: *	Ex. format: ip   url   useragent   referer
	Know more about Splunk Field / Index Name Configuration
Account Activation Email ID: *	Please enter Email-ID
	Email used for licensce activation and bot insight alerts
Promotional Code:	Promo Code(optional)
	Clear Save

- **7** Navigate to Apps > Radware Bot Risk Scanner > Configuration.
  - Source Index Name specify the Splunk index containing your application's access logs or web server logs for analysis.
  - Source Field Name Input Field from The Source Splunk Index [Field Format: IP | URL | user agent | referrer URL]
  - **7** Email ID Email ID is required to activate the license.
  - Promotional Code This is an optional field, and if you require additional traffic to be processed/month, send your request to <u>brs@radware.com</u> and we will share unique promotional code to extend your limit.

**Note:** The IP, URL and User Agent parameters are mandatory whereas the Referrer URL parameter is optional.

Once configured, the saved search will run every hour, and the dashboard will be ready within an hour.

Configuration	
Source Index Name: *	splunk_5449_data
Source Field Names: *	rpsbd&irpsbd#irpsbd7irpsbd3
	Know more about Splunk Field / Index Name Configuration.
Account Activation Email ID: *	-dherinkudescheme som
	Email used for licensce activation and bot insight alerts
Promotional Code:	Promo Code(optional)
	Clear Configuration Saved! Your Dashboard will be ready in 1 hour



# POST-INSTALL RECOMMENDATIONS

To process more than 50K records, you need to replace the "limits.conf" file in the following path. You can download the "limits.conf" file from the <u>following link</u>.

\$SPLUNK\_HOME/etc/apps/RadwareBotRiskScanner/local/limits.conf

- Once Radware Bot Risk Scanner is installed, it is advised to force a refresh of Splunk Configurations.
  - → For example, if your Splunk server is named Splunk and is running on port 8000, you would use the following URL: *http://<splunk:8000>/en-US/debug/refresh*
- **7** Also, it is recommended to clear the cache before using Bot Risk Scanner.
  - ➔ For example, if your Splunk server is named Splunk and is running on port 8000, you would use the following URL: *http://<splunk:8000>/en-US/\_bump*
- To check if the app is Enabled, navigate to Apps> Manage Apps and change the status to enabled|disable.

Apps						Browse more ap	ps Install app from file Create app
Showing 1-23 of 23 items							
filter Q							25 per page 💌
Name 🕈	Folder name 🕈	Version \$	Update checking \$	Visible \$	Sharing 🕈	Status 🕈	Actions
Radware Bot Risk Scanner	RadwareBotRiskScanner	1.0.4	Yes	Yes	App   Permissions	Enabled   Disable	Launch app   Edit properties   View objects

To Validate if the saved search is created properly, Navigate to Settings > Searches, Reports, and Alerts. You should find "Bot Risk Scanner Saved Search".

	Searches, Reports, and Alerts New Federated Search New Report New Alert Searches, reports, and alerts are saved searches created from pivot or the search page. Learn more ta											
1	Searches, Reports, and Alerts Type: All	<ul> <li>App: Radware Bot Risk Scanne</li> </ul>	er (Rad	wareBotRis	kScanner) • Owner: Admin	istrator (saivijayr) 👻	filter	Q				10 per page 🔻
	Name \$	Actions	4	Туре	Next Scheduled Time \$	Display View \$	Owner \$	App \$		Alerts \$	Sharing \$	Status \$
	Bot Risk Scanner Saved Search Search created on: 11/23/2022, 5:06:44 PM	Edit • Run 12 View Recent 12		Report	2022-11-23 12:01:00 GMT	none	saivijayr	RadwareBotRis	Scanner	0	Арр	✓ Enabled



Edit Search	$\mathbf{x}$
Title	Bot Risk Scanner Saved Search
Description	Search created on: Tue, 16 Jul 2024 11:18:32 GMT
Search	<pre>(earliest=-1h@h index=test_bvs latest=@h)   convert timeformat="%Y-%m-%d" ctime (_time) AS date   convert timeformat="%H" ctime(_time) AS hour   convert timeformat="%M" ctime(_time) AS minute   eval Eua=if( len(useragent) &lt;= 1, 1, 0 )   eval Kua=if( like( useragent, "%bot%") or like( useragent, "%http%"), 1, 0 )   eval ref = replace(referer,"//", "")   rex field=ref " (?<pref>/.*)"   eval URef=if(url=Pref, 1, 0 )   eval Eref=if( len(referer) &lt;= 1, 1, 0 )   stats count(ip) as totalhits, dc(minute) as umin, dc(referer ) as Dref, sum(Eref) as Eref, sum(URef) as URef, dc(url) as Durl, dc (useragent) as Dua, sum(Eua) as Eua, sum(Kua) as Kua by ip, date, hour   join ip type=left [   search index=test_bvs earliest==1h@h latest=@h   top useragent by ip limit=1   rename count as TuaCount]   join ip type=left [   search index=test_@s areliest==1h@h latest=@h   top url by ip limit=1   rename count as TurlCount]   join ip type=left [   search index=test_bvs earliest==1h@h latest=@h   top referer by ip limit=1   rename count as TrefCount ]   fields - url, useragent, referer, percent   rename ip as address   getbrs inputfield=address   spath input=BRSResponse   fields - BRSResponse   collect index=radware_brs_result</pref></pre>

Navigate to Action > Edit > Edit Search to review the search query and validate if the below query is generated with your input field.

( 🔩



## DASHBOARD & KPI DETAILS

The dashboard provides the following visualizations and key KPI Trackers:

Total Request: Total traffic in the Source Index scanned by Radware Bot Risk Scanner

**Bot Requests:** Total traffic classified as bots (Includes Crawler and Aggregator) by Radware Bot Risk Scanner.

**Bot Signature Count:** Total number of unique signatures created against bots (Includes Crawler and Aggregator) by Radware Bot Risk Scanner.

Total Requests	Bot Requests	Bot Signature Count
55,958,937	23,773,284	39,739

Impacted URL's: Total number of URL's being impacted by Bot Attacks

**Avg. Attack Duration | Top 10 IP's:** Average time spent by top 10 IP Address while performing Bot attacks.



Bot Traffic Trend: Bot traffic trend per hour classified by Radware Bot Risk Scanner.







**Bot Classification:** Types of bots classified by Radware Bot Risk Scanner.

Crawler Stats: Total traffic classified as Crawlers by Radware Bot Risk Scanner.



Aggregator Stats: Total traffic classified as Aggregators by Radware Bot Risk Scanner.





**Top Attack based on IP Address:** List of IP's classified as bad by Radware Bot Risk Scanner along with ISP, City, Country, and Total hits made by individual IP within the selected period.

Top Attack based on IP A	Address				
IP_Address \$	ISP \$	City ‡	Country \$		BadBotHits ≎
52.13.138.225	Amazon.com	Boardman	United States of America		5543
44.226.39.139	Amazon.com	Boardman	United States of America		5312
44.231.121.60	Amazon.com	Boardman	United States of America		5267
5.64.238.10	Sky Broadband	Darlington	United Kingdom of Great Britain and Northern Ireland		4899
178.250.7.64	Criteo SA	Paris	France		4622
178.250.7.70	Criteo SA	Paris	France		4455
178.250.7.68	Criteo SA	Paris	France		4400
89.249.109.177	Financijska agencija	Zagreb	Croatia		4395
178.250.7.74	Criteo SA	Paris	France		4307
178.250.1.83	Criteo SA	Paris	France		3659
				« Prev 1 2 3 4 5 6	7 8 9 10 Next »

**Top 10 URL's Impacted by Bots:** List of the top 10 URL's and the number of bad bot hits on each URL within the selected period.

Top 10 URL's Impacted by Bots	
URL \$	BadBotHits ≎
ROUT AND ADDRESS IN NORTH YORK	150844
$\label{eq:constraint} Wipold and the physical set of the second second$	37395
https://www.tjulialis.https://mapramtalyriwary.psi.itg	26337
10301-000-004030-00300-0040-0040-0040-00	23478
Hispochines a particular in Annala (a send participant) and a figure (cancel and in Coll Hispanye )	23470
https://www.tjutule.https://oppenditu/sect-upp factor fungerplatel	13793
ROLL Your Advands IN York	9562
Nips. Alex. Apalala in Sppi Appendia (ao esti sonieti sina basini Spenitedii infanisi)	4636
https://www.tjulials.https://pages/base.auto.text	4539
ROBIL/Yeek-Adabasis/Winede-Adabasis/Techt/WCD-agasit/WCD-roganit	4458

**Top 10 Referrer URL's Impacted by Bots:** List of top 10 Referrer URL and the number of bad bot hits on each URL within the selected period.

Top 10 Referrer URL's used by Bots	
Referrer ‡	BadBotHits ≎
	169836
$M_{\rm eff} = M_{\rm eff} = M_{e$	3489
https://www.spainda-te/ncjanglainda/private/ingjanglaint/intellingjant	3466
https://www.sjustala.ht/wjw-sjustala/pri.estaineji-sglasi.httlivel-sglasi	1901
Internet/Verse operiods. No/	926
https://www.sjustala.ht/wjw-sjustala/pedareti/wji-sglasi.httliwi-sglasi	726
https://www.google.com/	516
hidges/laws.sjudials.ht/witerialm	141
Inter-Viol Steen performentation	134
hidigan Alama Alpathalan An Angesi na Anmaian iar	124



#### Top 10 User Agents Bots:

Top 10 User Agents Impacted by Bots	
Useragent \$	BadBotHits 🗘
Mozilla/5.0 (Linux; Android 10; K) AppleMebKit/537.36 (0HTML, like Gecko) Chrome/113.0.0.0 Mobile Safari/537.36	40565
CritesBot/0.1+(+https://www.criteo.com/criteo-crawler/)	17196
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36	14060
ias-sg/3.3 (former https://www.admantx.com + https://integralads.com/about-ias/)	6123
ias-jp/3.3 (former https://www.admantx.com + https://integralads.com/about-ias/)	6114
ias-te/3.3 (former https://www.admantx.com + https://integralads.com/about-ias/)	5869
ias-or/3.3 (former https://www.admantx.com + https://integralads.com/about-ias/)	5682
ias-va/3.3 (former https://www.admantx.com + https://integralads.com/about-ias/)	4624
Mozilla/5.0 (Mindows NT 10.0; Min64; x64) AppleMebKit/537.36 (MMTML, like Gecko) Chrome/113.0.0.0 Safari/537.36 Edg/113.0.1774.57	3715
Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, 11ke Gecko) Chrome/111.0.0.0 Mobile Safari/537.36	3572

#### **Global Distribution & Top 10 City Based on Attack:**



**Note:** Exporting data from panels is disabled in the dashboard. To export data from a particular panel, hover over the bottom right corner of the panel and click on "Open in Search." The result will open in a new window without any additional query execution cost. A sample is shown below.





( 🥿

New Search		Save As  Cre	ate Table View Close
<ol> <li>International contents (e.g., and all contents ( contents contents) and all contents ( contents contents contents) and all contents ( contents contents) and all contents (</li></ol>	<pre>into record_const_inex_i transferrent_cons const, "Constant, congregation="const, log bot_brack_trappents" of _TextBells") attagents contr*_congregation() op result</pre>	ognaat an tomo y reganie <sup>1</sup> giniender + Willie	Custom time • Q
23,368 events (6/23/23 6:00:00.000 AM to 6/23	/23 12:00:00.000 PM) No Event Sampling •	Job 🕶 II 🔳 🦽 🚭	≱ _ ∮ Fast Mode ▼
vents Patterns Statistics (6) Visualiza	ation		
100 Per Page 🔹 🖌 Format 🛛 Preview 👻			
_time ‡	Aggregator 🗢 🖌	Bad Bots 🗢 🖌	Crawler \$
023-06-23 06:00	18624	54471	103834
023-06-23 07:00	23467	53634	118145
1023-06-23 07:00 023-06-23 08:00	23467 22529	53634 50541	118145 114717
023-06-23 07:00 023-06-23 08:00 023-06-23 09:00	23467 22529 21414	53634 50541 64431	118145 114717 82447
2023-06-23 07:00 2023-06-23 08:00 2023-06-23 09:00 2023-06-23 10:00	23467 22529 21414 22633	53634 50541 64431 58054	118145 114717 82447 51826

©2024 Radware Ltd. All rights reserved. The Radware products and solutions mentioned in this document are protected by trademarks, patents and pending patent applications of Radware in the U.S. and other countries. For more details please see: <u>https://www.radware.com/LegalNotice/</u>. All other trademarks and names are property of their respective owners.