

IP Spotlight

Overview

IP Spotlight is a threat analytics tool that allows you to expose and inspect information about a specific IP address gathered by StackPath's vast network of traffic. This information allows you to gather insights about the clients that access your sites, which will help you to make more educated decisions when creating WAF Rules that help to prevent and mitigate attacks.

The IP Spotlight feature provides information such as the source of an IP, its total number of requests, destinations, Whois data, and any malicious activity the IP has engaged in against other sites across our platform.

IP Risk Score

StackPath queries multiple external and internal databases in order to retrieve and store information about an IP address, which gives IP Spotlight the ability to provide a Risk Assessment and Score related to the IPs' threat level. Ranging from Low to Extreme, this score allows you to determine what actions should be taken against any flagged IP making requests to your site.

In addition, the WAF will begin automatically blocking requests as soon as threats are detected based on this score.

A higher risk score is typically assigned to IPs that exist on external block lists, participate in DDoS attacks, or make higher numbers of requests than usual.

Available Data

Below is a list of the available data for IP addresses provided by our IP Spotlight feature:

- Whois information
- Risk score
- Tags
- Request count
- Total request count for a specific IP where the result field is blocked
- Distinct count of sessions
- Top 10 user agents for the IP
- List of countries that were attacked by this IP
- Time series data of blocked requests by "attack type"
- DDoS information
- Total request count for a specific IP and specific site

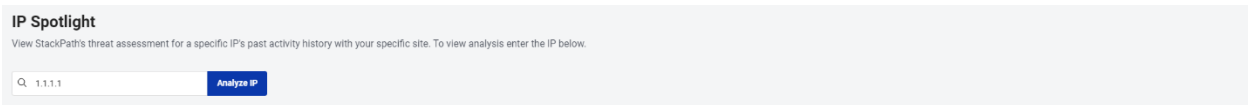
- Total request count for a specific IP where the result field is blocked for a specific IP and a specific site
- Distinct count of sessions for a specific IP and a specific site
- Top 10 URLs accessed by an IP to a specific site
- Information about the top sessions from an IP to a specific site
- A break down of attacks by rule name and sanction

Navigating the Portal

This section will walk you through the IP Spotlight settings and features shown in the Control Portal.

Analyze IP

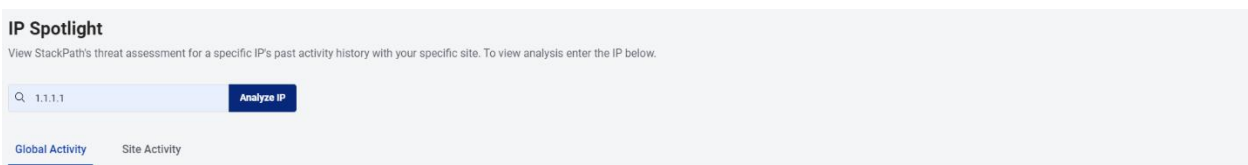
Enter the IP address that you would like to analyze here.



The screenshot shows the 'IP Spotlight' section of the Control Portal. It includes a search bar with the IP address '1.1.1.1' entered and a blue 'Analyze IP' button to its right. Below the search bar is a small line of text: 'View StackPath's threat assessment for a specific IP's past activity history with your specific site. To view analysis enter the IP below.'

Global Activity

The data displayed in the **Global Activity** tab is built from the generic IP information gathered, as well as the information we gathered from all other users on our platform. This is more aggregate in nature.



This screenshot shows the 'IP Spotlight' interface with the 'Global Activity' tab selected. The search bar contains '1.1.1.1' and the 'Analyze IP' button is visible. Below the search bar, there are two tabs: 'Global Activity' (which is active and underlined) and 'Site Activity'.

IP Threat Summary

The **IP Threat Summary** section will provide you with the following details as they relate to our platform as a whole:

- The IP's Risk Assessment score
- Total number of requests
- Number of requests blocked
- Number of unique sessions
- Use of Botnets
- What the IP is known for

IP Threat Summary / 1.1.1.1			RISK ASSESSMENT: NO RISK
Total Requests	Requests Blocked	Unique Sessions	
0	0	0	
Use of Botnets	Known For		
No	knowbot		

Whois

The **Whois** section will provide the Whois information for the IP. This information is pulled from the global Whois database.

Whois / 1.1.1.1

Country	AU	IP Range	1.1.1.0-1.1.1.255
Organization	APNIC Research and Development	Owner Type	hosting services

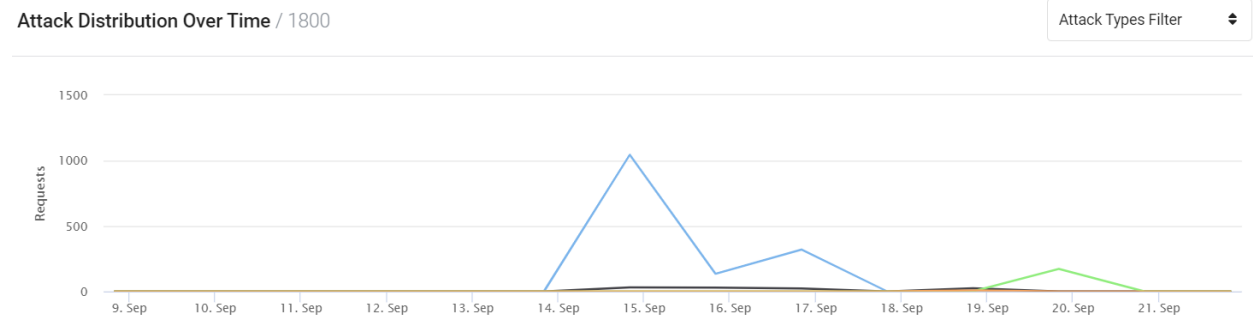
Top Ten Attack Targets

This section displays a map that marks the origin and targets of any attack associated with the IP.



Attack Distribution Over Time

This section displays a graph containing the number of blocked requests filtered by the policy that was triggered.



Site Activity

The data displayed in the **Site Activity** tab contains more detailed information about your specific domain. Select the site you want to analyze from the drop-down menu.

IP Spotlight
View StackPath's threat assessment for a specific IP's past activity history with your specific site. To view analysis enter the IP below.

Q 1.1.1.1 Analyze IP

Global Activity Site Activity

Overview

The **Overview** section will provide you with the following details as they relate to your specified site:

- Total number of requests
- Number of requests blocked
- Number of unique sessions

Total Requests

3000

Requests Blocked

3000

Unique Sessions

2086

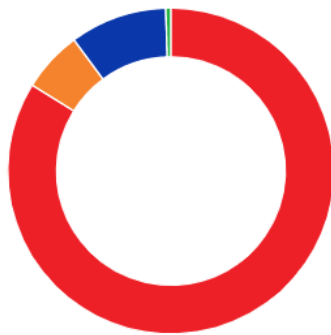
Actions Taken Per Rule

This section will provide you with a dropdown of all rules applicable to this IP and graph displaying how many times each rule was applied.

Actions Taken Per Rule

4 of 4 Selected

Rules



Automated Clients

1509

Force Browser Validation on Traffic Anomalies

109

Obfuscated Attacks and Zero-Day Mitigation

173

XSS Attack

9

Top 10 URLs Visited

This section displays a list of the top 10 URL paths visited along with the number of times these URLs were requested.

URL PATH	REQUESTS
/	2316
/%%3cscript%%3ealert...	225
/select * from	156

Top 10 Sessions

This section contains a table displaying information on the top 10 sessions from the specified IP. Included in this table are the Session ID, date the session took place, the TTL of the request, whether or not it was blocked and the session duration.

SESSION ID	DATE	REQUESTS	BLOCKED	DURATION
cc88b5536f0c...	Mon, Sep 19, 2022, 9:11:52 PM	130	130	1 second
cc88b5536f0c...	Mon, Sep 19, 2022, 9:11:52 PM	151	151	1 second
e6ed56d70782...	Tue, Sep 20, 2022, 8:28:35 AM	98	98	3 seconds
e6ed56d70782...	Tue, Sep 20, 2022, 8:28:35 AM	98	98	3 seconds

Want More Info?

You might find these articles helpful to get started using StackPath WAF and IP Spotlight:

- [WAF Package Offerings](#)
- [Allowing and Blocking IP Addresses](#)
- [IP Reputation](#)

If you have any questions, or want more information regarding IP Spotlight please [contact Support](#).