ThreatRadar Bot Protection Services

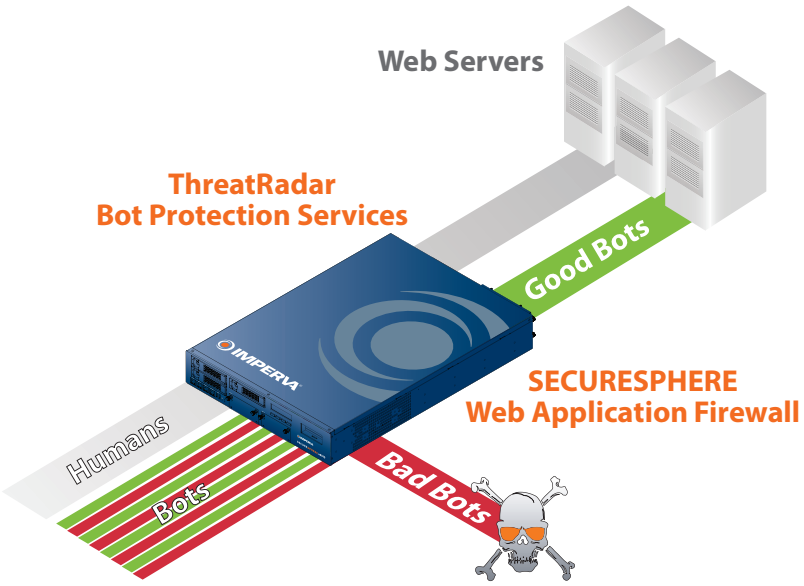
Improve Website Security and Performance by Eliminating Malicious Bots

Benefits

- Improve web application security by blocking malicious bots
- Improve website performance by eliminating unwanted/unwelcome bots, which account for up to 30% of all website traffic
- Classify and respond to clients by type: good bots, bad bots and human users
- Allow legitimate bots, such as Google and Bing, to access your website unimpeded

Over half of all website traffic is not from human users at all; it is from bots. These bots, such as search engine crawlers, are harmless; others are more nefarious. They are probing sites, scraping web content, posting spam messages, or attacking websites. Malicious bots account for more than 95% of all website attacks, including DDoS attacks, injecting comment spam, and scraping website content.

ThreatRadar Bot Protection Services is an add-on service for SecureSphere Web Application Firewall that accurately distinguishes between good bots, bad bots, and human users, so you can take action accordingly. Using SecureSphere WAF and ThreatRadar Bot Protection Services, malicious bots, a top threat for web applications, can be identified and stopped.



Good Bots

These are bots for monitoring search engine and website health that are operated by well-known and commonly-used services. ThreatRadar Bot Protection Services' client classification engine identifies these legitimate bots, and allows them to access your site.

Bad Bots

These include comment spammers, SQL Injection worms, vulnerability scanners and other known malicious bots. Bad bots are automatically blocked by ThreatRadar Bot Protection Services which stops them from attacking your website.

Suspected Bots

There are a huge number of bots on the web being used for various purposes. Unwanted bots generate redundant load on the web server, pose the risk of scraping and content theft, while not adding any value to the website itself. ThreatRadar Bot Protection Services provides an easy-to-use tool to stop these bots from accessing the website using the suspected bot setting.

Bot Access Control

ThreatRadar Bot Protection Services' client classification engine analyzes and classifies all incoming traffic to your site. This engine distinguishes between human and bot traffic, identifies "good" and "bad" bots, classifies traffic by browser type, and more. This granular level of information enables you to control who is allowed access to your website.

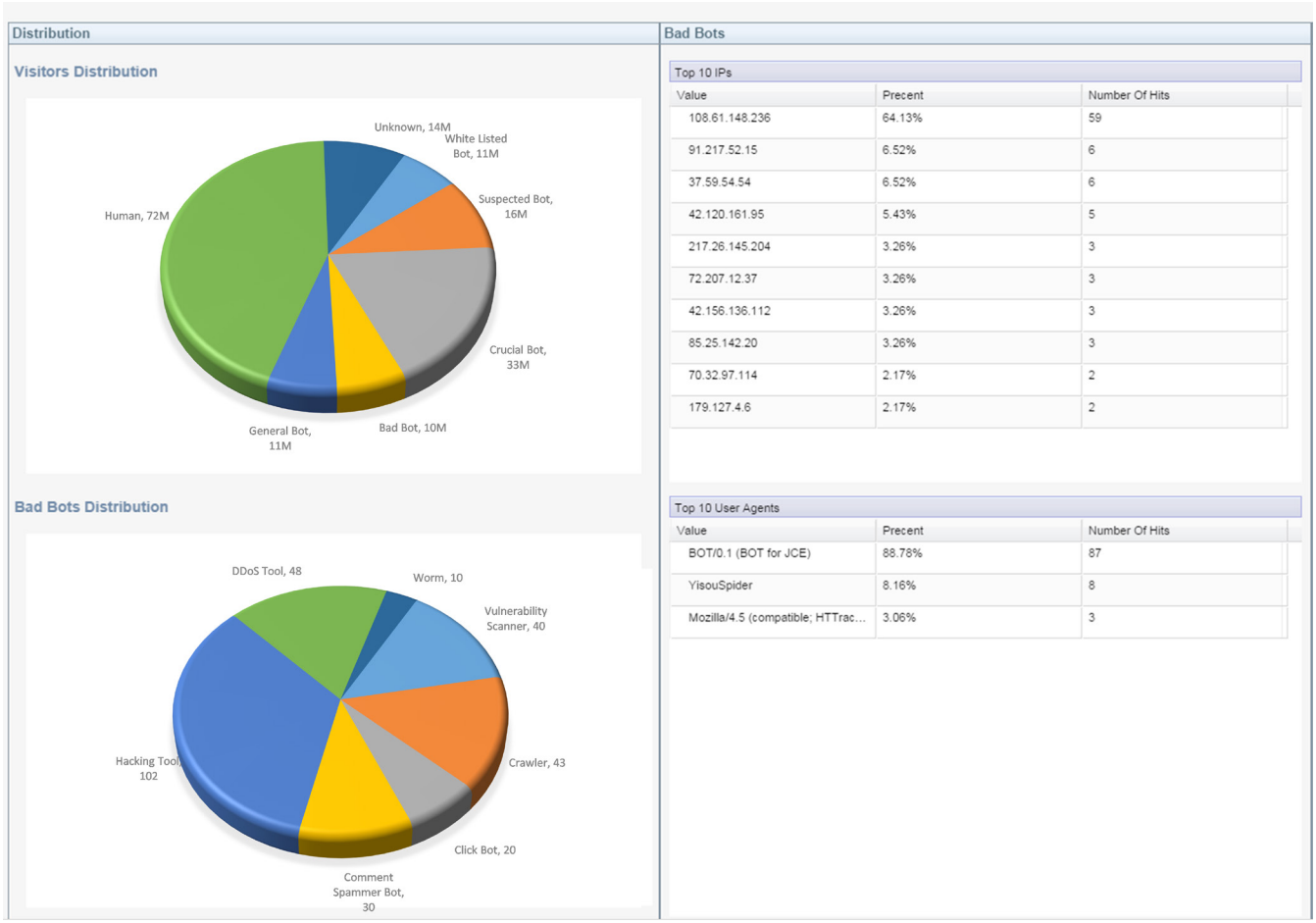
This classification information is used to drive WAF policy enforcement decisions, including handling bad and suspected bots. You can choose to have administrators receive an alert (e.g., for monitoring purposes), or have SecureSphere block the bot.

Dedicated Security Rules for Known Vulnerabilities

Imperva monitors hacker activity, hacker communications, and zero day exploits, in order to make sure that websites using our Bot Protection Services are protected.

Detailed Threat Analysis

ThreatRadar provides a detailed analysis of every threat that was posed to your website including: IP address, user agent, location, and other session information.



IMPERVA®

www.imperva.com