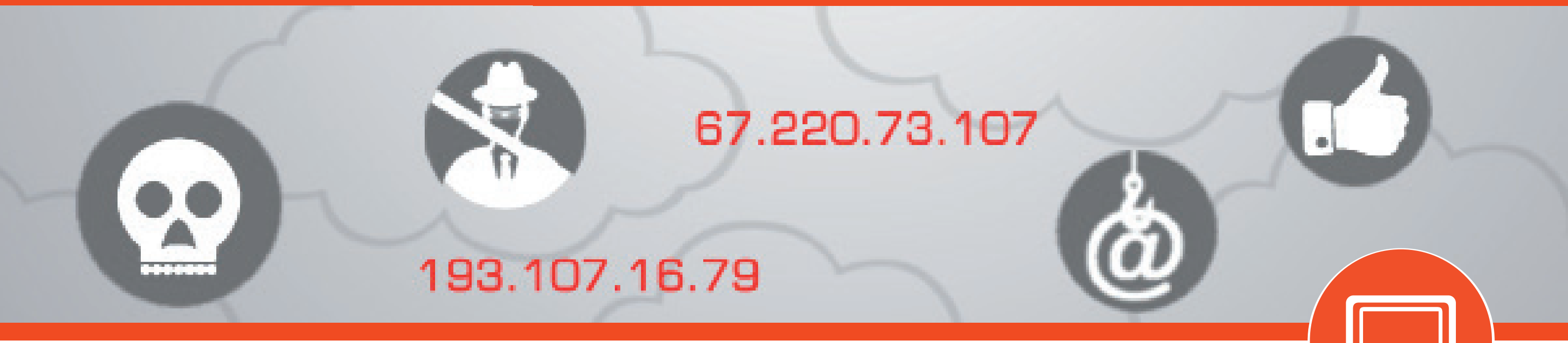
denyall
a Rohde & Schwarz Cybersecurity company

IP REPUTATION SERVICE



- + *Real-time*
- + *Accurate*
- + *Actionable*

POWERED BY WEBROOT

IP Rep

8 REASONS TO CHOOSE DENYALL IP REPUTATION SERVICE

1. **Global threat intelligence**: monitors +4B IP addresses, +27B URLs, +20B mobile apps and +600M email domains to evaluate the risk associated with source IPs, globally.
2. **Near real-time:** the database is updated every 5 minutes. Your WAF works with up-to-date intelligence on potentially malicious IP addresses.
3. **Reputation score:** based on historical & contextual data, the score evaluates the risk associated with any given IP address.
4. **Threat categories:** program your WAF to appropriately handle requests coming from IPs used by scanners, spies and spammers.
5. **Accurate:** the list, categories and score are updated so you rely on information that is more current than what static blacklists provide.
6. **Dynamic:** 100 000 new IP addresses are added and 38% of IPs are removed from the database every day.
7. **Actionable:** the IP reputation score and category information consumed by your DenyAll WAF helps handle attacks more effectively.
8. **User behavior:** IP reputation is a great data source for DenyAll's User Reputation Scoring engine to assess the trustworthiness of users.

ADD IP INTELLIGENCE TO YOUR WEB APPLICATION FIREWALL

The DenyAll IP Reputation Service brings up-to-date, actionable threat intelligence to WAF administrators charged with fending off modern-day application layer attacks. The service is powered by Webroot's Threat Intelligence platform, a cloud-based big data engine that **automatically analyses** and correlates feeds from millions of sensors distributed globally in real time.

DenyAll IP Reputation Index

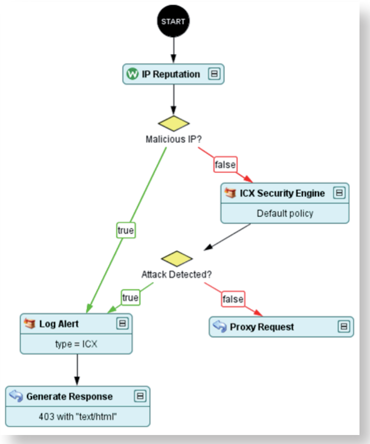
HIGH RISK	✋	01-20	These are high risk IP addresses. There is a high predictive risk that these IPs will deliver attacks – such as malicious payloads, DoS attacks, or others – to your infrastructure and endpoints.
SUSPICIOUS	!	21-40	These are suspicious IPs. There is a higher than average predictive risk that these IPs will deliver attacks to your infrastructure and endpoints.
MODERATE RISK	–	41-60	These are generally benign IPs but have exhibited some potential risk characteristics. There is some predictive risk that these IPs will deliver attacks to your infrastructure and endpoints.
LOW RISK	✓	61-80	These are benign IPs and rarely exhibit characteristics that expose your infrastructure and endpoints to security risks. There is a low predictive risk of attack.
TRUSTWORTHY	✓	81-100	These are clean IPs that have not been tied to a security risk. There is very low predictive risk that your infrastructure and endpoints will be exposed to attack.

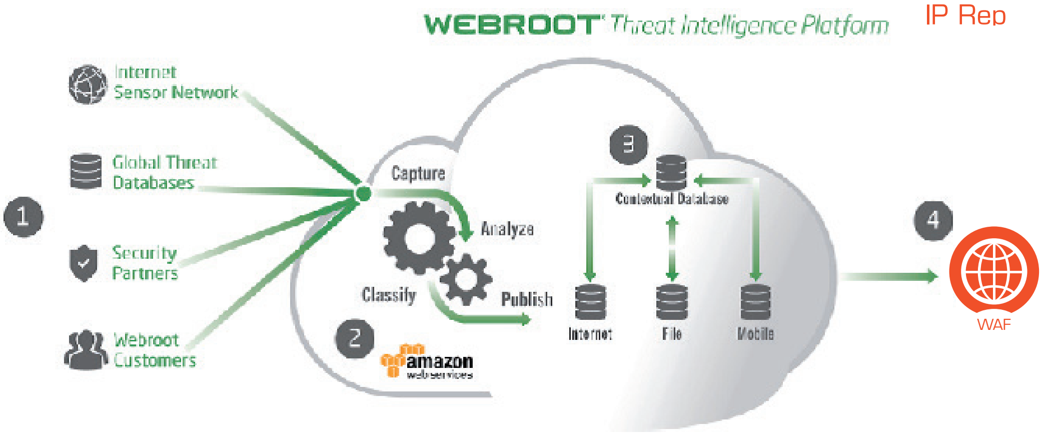
The DenyAll IP Reputation Service delivers up-to-date and accurate reputation score and categorization for over 12 million dangerous IP addresses in near real-time. It integrates seamlessly with DenyAll's Web Application Firewalls to optimize the performance of your WAFs, **reduce the number of false positives**, block malicious bots as early as possible and adjust the authentication and security policies based on user context and behavior.

denyall
a Rohde & Schwarz Cybersecurity company

IP REPUTATION SERVICE

IP Rep





DENYALL IP REPUTATION SERVICE USE CASES

Performance Optimization

- Don't filter requests originating from IP sources known to be malicious with a high degree of reliability
- Filtering them would likely result in a 'block' decision
- Reduce the burden on your WAF by dropping such requests without even filtering them.

Lower the risk of false positives

- Lower the risk of false positives by adjusting the policy based on the origin of the requests.
- A less stringent security policy can be used when requests originate from trusted IP addresses.
- A more demanding policy can be applied to all requests originating from IP addresses with a less trustworthy score or belonging to a questionable category.

User reputation evaluation

- Prevent users from misusing their rights and attacking the application, even if they connect from safe IPs.
- Block requests from users connecting from safe IPs who attack the application or misuse their rights.
- Adjust response strategy to situations where legitimate user is connecting from questionable IP.

Bad bots limitation

- Block malicious bots based on threat intelligence data
- Disregard requests coming from IP addresses associated with malicious bots such as spammers, phising sites, Windows exploits or infected enpoints
- Limit the traffic rate of other bots, such as crawlers and requests coming out of proxy networks.

Adaptive authentication

- Adjust authentication policy to IP source context based on intelligence
- Require stronger authentication from users connecting from less trustworthy IP sources based on the IP addresses' reputation score, or taking into account whether an IP address is associated with a particular threat category you want to treat with special care (like proxies, for example).

Adjust to new scenarios

- Adjust your security and authentication policies to a changing threat landscape.
- DenyAll IP Reputation Service is compatible with DenyAll i-Suite 5.5.12, DenyAll WAF 6.4 and rWeb 4.2.4 and more recent versions.

ABOUT DENYALL

DenyAll is a software vendor, expert in application security. For 15 years, we have been helping demanding customers secure their web applications and services. Our products detect IT vulnerabilities, protect infrastructures against modern attacks targeting the application layer and connect users to the applications which allows them to create and share information. In 2017, DenyAll was acquired by Rohde & Schwarz Cybersecurity.

6 avenue de la Cristallerie 92310 Sèvres - FRANCE

☎ +33 (0)1 46 20 96 00
📠 +33 (0)1 46 20 96 02

✉ info@denyall.com
@ www.denyall.com

ROHDE & SCHWARZ
Cybersecurity