WEBROOT
Smarter Cybersecurity™

BrightCloud® IP Reputation Service

Enhance customer defenses with dynamic IP reputation intelligence to stop IP threats before they cause damage

Overview

- Every packet on the internet has a source and a destination IP address
- Disabling communication from malicious IPs is effective but difficult without highly accurate, predictive threat intelligence
- The Webroot BrightCloud® IP Reputation Service provides up-to-the-minute IP intelligence, enabling technology partners to better protect their customers' networks

Today, cybercriminals have an immense number of exploits and attack vectors available, and they use numerous techniques to hide their identities and activities, such as encrypted communications, DNS cache poisoning, URL redirection, hyperlink obfuscation, etc. Disabling inbound communications from IPs known to be malicious, which have associations with other malicious online objects, is a highly effective way to keep networks secure.

IP addresses are not static and may cycle from malicious to benign and back multiple times. In 2018, Webroot found that 40% of bad IP addresses showed malicious activities more than once. However, many publicly available lists are static and outdated.[1]

The BrightCloud IP Reputation Service helps technology partners augment their customers' security by adding a dynamic IP reputation service to their defenses. Webroot provides a continuously updated feed of known malicious IP addresses broken down into 11 categories so IT security administrators can easily identify threats by type and protect their networks. These categories are: Windows Exploits, Web Attacks, Phishing, Botnets, Denial of Service, Scanners, TOR Proxies, Anonymous Proxies, Reputation, Spam Sources, and Mobile Threats.

With this service, customers gain dramatic improvements in security efficacy and efficiency, as the time required to identify IP threats is drastically reduced. The service also provides information such as historical and geolocation data to help security admins make better, more proactive threat decisions.

The BrightCloud IP Reputation Service is powered by the Webroot® Platform, which uses a big data architecture to provide the most comprehensive and accurate threat intelligence available today, including up-to-the-minute intelligence on IPs of emerging threats. This includes a dynamic list of approximately 6 million dangerous IPs at any given time. This intelligence can be used to block traffic from TOR nodes, proxies, botnets, and other malicious actors.

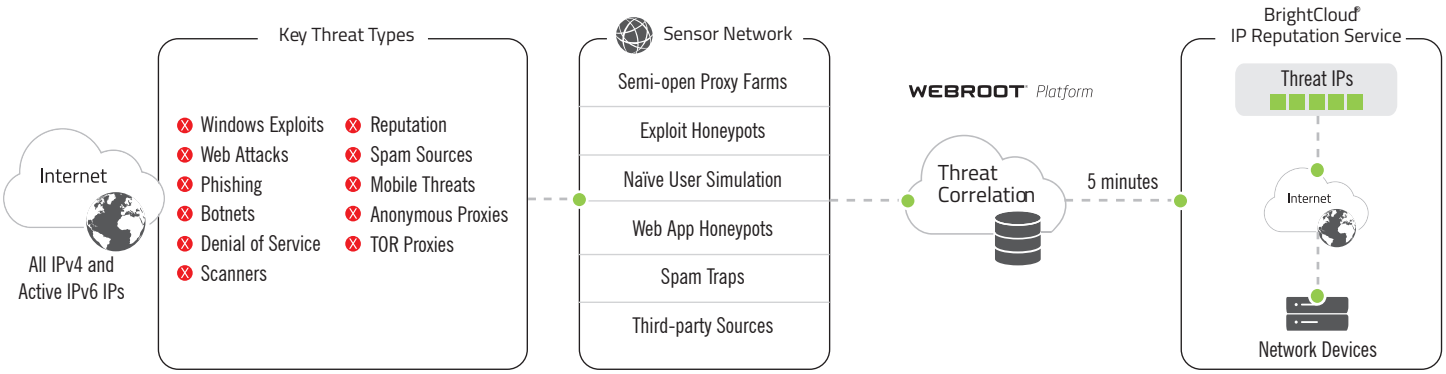
Customers can also access a rich set of metadata for investigative purposes. For example, proxies have been used for more than just obfuscation, but also to launch short span DDoS attacks. Similarly, botnet command and control contains BOT IPs as well as the originating central server IP. In addition, add-on IP Threat Insights provides supplementary evidence of why an IP was tagged as malicious, including the type(s) of malware it distributed, ports and protocols used, and the time span that it posed a threat.

The Webroot Platform analyzes and correlates data to create a predictive risk score, which falls into one of five rating bands ranging from trustworthy to malicious. The BrightCloud IP Reputation Index provides scores ranging from 1 to 100, with tiers split into Trustworthy, Low Risk, Moderate Risk, Suspicious, and High Risk. Numerically lower scores indicate IPs that are more likely to be or become bad, and are monitored at a greater frequency than trustworthy IPs.

BrightCloud IP Reputation Index

01-20 High Risk	**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.**
21-40 Suspicious	**These are suspicious IPs. There is a higher than average predictive risk that these IPs will deliver attacks to your infrastructure and endpoints.**
41-60 Moderate Risk	**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.**
61-80 Low Risk	**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.**
81-100 Trustworthy	**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.**

[1] 2019 Webroot Threat Report, February 2019



Webroot BrightCloud® IP Reputation Service

The reputation tiers enable enterprises to finely tune their security settings based on their risk tolerance and business needs. This enables them to proactively prevent attacks by limiting the exposure of their networks to dangerous or risky IPs. For example, a highly security conscious bank may choose to block anything with a score lower than 80, while others may choose to accept traffic from IPs with scores higher than 60 as long as the site being accessed is affiliated with a partner.

Partner Benefits

» **Differentiate yourself from your competition**
Offer your customers industry-leading protection against approximately 6 million malicious IPs at any given time

» **Minimize false positives**
Harness the world's most powerful cloud-based security analysis engine

» **Easy to integrate, easy to use**
Simple integration into your solution via RESTful API, STIX, and an SDK

» **No impact on your network**
Protects through your network devices and increases user capacity by eliminating unwanted traffic

BrightCloud IP Reputation in Action

To keep the list updated and accurate, Webroot uses a detention methodology to evaluate IPs. The service:

» Deploys an automated algorithm to identify suspicious IPs
» Examines and correlates by the IP
» Applies built-in rules to test the IP
» Determines if and how long to restrict the IP
» Releases the restrictions on the IP but keeps it under watch

This service not only enhances enterprise customers' abilities to counter IP threats, but also avoids the taxing security processing many other IP reputation services impose. It can be used to power an IP intelligence service in network perimeter appliances to block traffic from malicious addresses, protecting sensitive data. It can also be used to track known proxies, allowing customers to prohibit malicious requests from phishing sites, such as man-in-the-middle attacks, or to respond with an alert.

Easy Integration

Using our intuitive SDK, REST services, and API, technology partners can easily integrate BrightCloud services into their own solutions. The BrightCloud IP Reputation Service integrates with existing security solutions through the same SDK as other BrightCloud services, making integration of multiple services easy. For BrightCloud IP Reputation, the full database is downloaded to the endpoint with an update recommended every five minutes.

Our partners across the globe have had tremendous success integrating Webroot intelligence into their network solutions, from next-generation firewalls to network load balancers. Because Webroot provides an uncomplicated integration, this solution can be implemented simply and easily by network and security vendors worldwide.

About Webroot
Webroot was the first to harness the cloud and artificial intelligence to protect businesses and individuals against cyber threats. We provide the number one security solution for managed service providers and small businesses, who rely on Webroot for endpoint protection, network protection, and security awareness training. Webroot BrightCloud® Threat Intelligence Services are used by market leading companies like Cisco, F5 Networks, Citrix, Aruba, Palo Alto Networks, A10 Networks, and more. Leveraging the power of machine learning to protect millions of businesses and individuals, Webroot secures the connected world. Headquartered in Colorado, Webroot operates globally across North America, Europe, and Asia. Discover Smarter Cybersecurity® solutions at webroot.com.

World Headquarters
385 Interlocken Crescent
Suite 800
Broomfield, Colorado 80021 USA
+1 800 772 9383

Webroot EMEA
6th floor, Block A
1 George's Quay Plaza
George's Quay, Dublin 2, Ireland
+44 (0) 870 1417 070

Webroot APAC
Suite 1402, Level 14, Tower A
821 Pacific Highway
Chatswood, NSW 2067, Australia
+61 (0) 2 8071 1900