DATASHEET

BrightCloud® Threat Intelligence

BrightCloud® IP Reputation Service

Enhance customer defenses with dynamic IP reputation intelligence to stop IP threats

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 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 extremely dynamic, with many exhibiting both benign and malicious behavior over time or exhibiting different types of malicious behavior. When looking at the top 50k most recurring IPs in BrightCloud data during 2020, 97.3% of IPs were convicted in at least four categories throughout the year, such as spam sources or Windows exploits. Nearly 45% of the top 50K were convicted during at least 2 different months, with 25.8% of the top 50K found doing something malicious in all 12 months.[1]

The BrightCloud® IP Reputation Service supports operational security needs by providing a dynamic service to inform automation decisions and strengthen defenses. With a continuously updated feed of known malicious IP addresses, IT security administrators can easily identify threats by type to protect their networks and gain dramatic improvements in security efficacy and efficiency. This service integrates seamlessly and is tailored for your operational needs and use cases.

The BrightCloud IP Reputation Service is powered by the BrightCloud® 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 millions of emerging threats. This intelligence can be used to block traffic from TOR nodes, proxies, botnets, and other malicious actors.

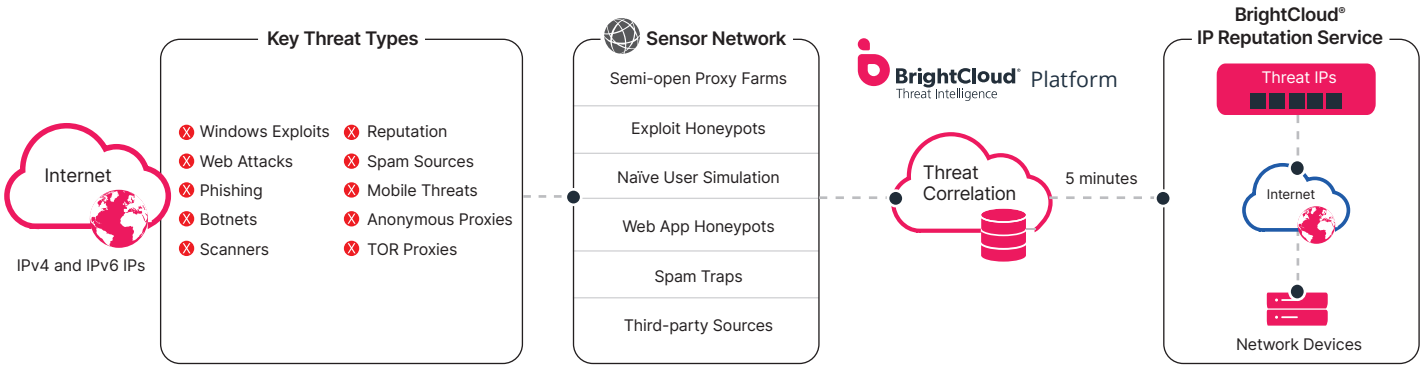
Customers can also access a rich set of metadata for investigative purposes. For example, proxies have been used for more than just obfuscation, but also to launch short span DDoS attacks. Similarly, botnet command and control contains BOT IPs as well as the originating central server IP.

The BrightCloud IP Reputation Service includes intelligence on all IPv4 addresses as well as in use IPv6 addresses. With our enhanced support of both threat and geo data for IPv6 addresses, partners can download data through an API call to receive additional threat information. As IPv6 adoption becomes more prevalent and IPv6 addresses are increasingly being used as an attack vector, having this additional data is critical in protecting the end user.

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.

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.

BrightCloud IP Reputation Index



BrightCloud® IP Reputation Service

The BrightCloud 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.

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 dynamic, industry-leading protection against millions of malicious IPs
- **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 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, BrightCloud 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 end users' 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 RESTful 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 BrightCloud intelligence into their network solutions, from next-generation firewalls to network load balancers. Because BrightCloud provides an uncomplicated integration, this solution can be implemented simply and easily by network and security vendors worldwide.

Contact us to learn more
BrightCloud.com
Phone: +1 800 870 8102

[1] 2021 Webroot BrightCloud® Threat Report

About BrightCloud

BrightCloud was the first threat intelligence platform to harness the cloud and artificial intelligence to stop zero-day threats in real-time. The platform is used to secure businesses and their products worldwide with threat intelligence and protection for endpoints and networks. With more than 10 years of experience in building and analyzing the industry's most robust internet threat database, BrightCloud has the strongest coverage model, fewest uncategorized objects and the most historical records which others cannot replicate.

In 2019, BrightCloud was acquired by OpenText, a global leader in Enterprise Information Management. As a whole, we are a market leader in cyber resilience, offering total endpoint protection and disaster recovery for businesses of any size.