BrightCloud IP Reputation Service

Stop ransomware and zero-day application attacks, phishing, botnets, and other web-based threats with comprehensive, up-to-the-minute IP reputation intelligence.

Challenge: Collecting, analyzing, and disseminating IP reputation threat data

IP reputation intelligence is a critical strategic resource for cybersecurity providers. Comprehensive, reliable data about IP addresses enables IT security solutions to disable communications with malicious and suspicious systems on the internet. With accurate data, solutions can block ransomware and zero-day application attacks, thwart phishing campaigns, throttle botnets and DDoS attacks, and defeat other web-based threats. Contextual information about IP addresses can also help customer security teams quickly and accurately investigate and respond to attacks.

But cybersecurity providers face a massive challenge collecting, analyzing, and disseminating IP reputation intelligence. To be successful, they have to track billions of IP addresses and analyze tens of thousands of new ones every day. They contend with numerous techniques threat actors use to hide their identities and activities, such as encrypted communications, anonymous proxies, DNS cache poisoning, URL redirection, and hyperlink obfuscation. And they must collect and correlate metadata related to IP addresses. Since threat actors use hundreds of new IP addresses every hour, cybersecurity providers must deliver updated IP reputation intelligence to security solutions in minutes.

Solution: The BrightCloud IP Reputation Service

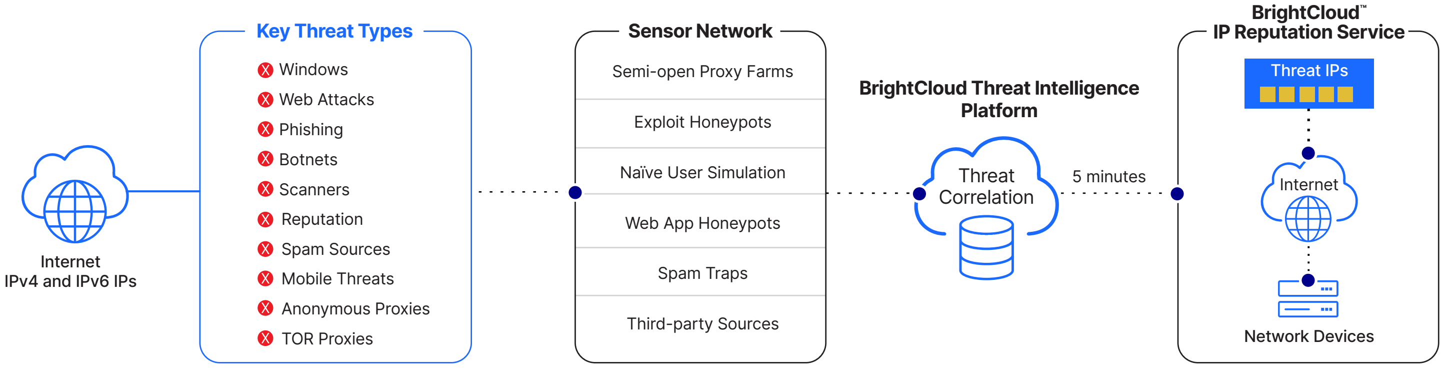
The OpenText™ BrightCloud™ IP Reputation Service provides a world-class operational intelligence solution for cybersecurity providers and their customers. BrightCloud's IP reputation service is:

- **Comprehensive**—Covering more than four billion IPv4 and IPv6 addresses on a given day, the BrightCloud IP blacklists contain about four million active bad IPs, with around 35,000 brand new malicious IPs detected daily.
- **Accurate**—Sixth-generation machine learning and massive data sets from millions of real-world sensors help identify malicious, suspicious IP addresses and minimize false positives.
- **Insightful**—A rich set of metadata provides insights for investigative purposes.
- **Up-to-the-minute**—The service updates IP reputation scores every five minutes.
- **Easy to integrate and use**—An intuitive RESTful API and SDK simplify integration with cybersecurity solutions and facilitate automated decision processes.

Product highlights

- Fine-tune security settings based on predictive risk scores.
- Rely on an IP reputation service that stays updated and accurate.
- Easily integrate BrightCloud with your current solutions.

BrightCloud is a proven leader in operational threat intelligence and a trusted partner to over 140 security leaders and innovators.



Key features

The BrightCloud IP Reputation Service is powered by the BrightCloud® Threat Intelligence Platform. Its big data architecture provides 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 to improve analytics and incident response. For example, metadata relating to observed attacks can help determine if an attack is targeted against a specific organization or is a more generalized, opportunistic attack.

Benefits

The BrightCloud IP Reputation Service includes intelligence on all public 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 used as attack vectors, having this additional data is critical for comprehensive detection.

In addition, the IP Threat Insights add-on provides supplementary evidence of why an IP was tagged as malicious. Evidence includes the type(s) of malware it distributed, ports and protocols used, associated malicious URLs, and the time span that it posed a threat.

Feature	Benefit
Global IP threat intelligence	Achieve worldwide IP threat visibility and analysis across millions of malicious IPs, plus detection of over 35,000 new threats daily.
Contextual awareness	Gain more insight into IP threat information for inbound and outbound traffic within your network to known malicious destinations and correlated threat insights.
Effective policy enforcement	Enforce policies based on specific attack vectors: e.g., prevent external communication to IPs of known command and control servers.
Advanced threat protection	Stop advanced cyberattacks like malware, ransomware, phishing, and command and control by leveraging IP intelligence with high confidence.

Predictive risk scores

The BrightCloud platform analyzes and correlates data to create a predictive risk score for each IP address. Scores range from 1 to 100, and are grouped into five rating bands: Trustworthy, Low Risk, Moderate Risk, Suspicious, and High Risk. IP addresses that are predicted to become malicious are monitored at a greater frequency than trustworthy IPs.

The reputation tiers enable users of partner solutions to fine-tune their security settings based on their risk tolerance and business needs. They can proactively prevent attacks by limiting the exposure of their networks to dangerous or risky IPs. For example, a security-conscious bank may choose to block anything with a score lower than 60, while others may choose to accept IPs with scores higher than 40, as long as the site is affiliated with a partner.

1-20 High risk	✋	These are high risk IPs. 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 generally 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 in action

To keep the IP reputation service updated and accurate, BrightCloud uses a prosecution and detention methodology. The service:

- Uses an automated algorithm to identify suspicious IPs.
- Examines and correlates data associated with each address.
- Applies built-in rules to test the IP and determine if and how long to restrict it.
- Minimizes false positives by continuously updating threat data.
- Establishes the monitoring frequency for the IP after the restriction is lifted.

This service not only enhances the enterprise's ability to counter IP threats, but it also avoids the taxing security processing of many other IP security services. The service can power network perimeter appliances to block traffic from malicious addresses, protecting sensitive data. It can also identify known proxies, which helps block malicious requests from compromised internet hosts.

Easy integration

Using BrightCloud's RESTful API, technology partners can easily integrate our services into their own solutions. The BrightCloud IP Reputation Service integrates with existing security solutions through the same SDK as other BrightCloud offerings, making integration of multiple services easy. For BrightCloud IP Reputation, the IP blacklists can be synchronized every five minutes.

Contact us to learn more.

BrightCloud.com

brightcloud-sales@opentext.com

[1] 2023 Webroot BrightCloud® Threat Report

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk. DS_120623