DATASHEET

BrightCloud®
Threat Intelligence

BrightCloud® Web Classification and Web Reputation Services

Real-time web threat intelligence accurately assesses URL and domain risk and helps enforce web policies

Overview

- Malicious URLs often hide in otherwise benign domains, rendering basic domain-level intelligence ineffective
- Increased use of HTTPS can leave end users susceptible to visiting malicious or unwanted URLs
- The BrightCloud® Web Classification and Web Reputation Services categorizes the largest URL database of its kind across 82 categories and scores website and domain risk, regardless of internet category
- These services enable technology partners' solutions to protect end users, set and enforce usage policies and secure organizations against legal liabilities around web usage and compliance

New websites and online threats have something in common: they both emerge at astonishing rates and often in concurrence. Traditional, static, list-based internet protection services are no longer up to the challenge these new sites and threats present. Dynamically generated web content, mashups, rapid deployments, website structure and links change very quickly, providing fertile ground for cybercriminals and creating a serious security gap. In addition, many websites don't have sufficient security, while others are specifically designed to take advantage of visitors. Internet users are exposed to phishing, keyloggers, spyware, drive-by malware and the many other types of malicious code, which are only increasing in prevalence as new websites appear. Even legitimate sites are compromised regularly, while others shift rapidly between malicious and benign to avoid detection. The increase in adoption of HTTPS protocols limits visibility to the domain level within devices that do not or cannot decrypt traffic. These devices are typically meant for home or small business use. They also can extend into the enterprise arena, which can make the impact widespread.

In 2020, approximately 1 in 10 malicious sites were hosted on a benign domain.[1]

The BrightCloud® Web Classification and Web Reputation Services offers today's technology providers the most effective way to help customers enforce web policies and secure their users against web threats. By using cloud-based analytics and the most advanced machine learning in the industry, BrightCloud services have scored and classified over 95% of the internet—more than 999 million domains and 43 billion URLs to date—to generate the largest URL database of its kind.

Web Classification

By providing the broadest, most up-to-date and accurate website intelligence, Web Classification significantly improves visibility into all internet usage. Additionally, with the superior coverage and visibility offered by this service, technology providers can address their customers' key concerns which may include: employee productivity, IT bandwidth resource utilization, legal liabilities around web usage and compliance. Using BrightCloud Web Classification, technology partners can help their customers mitigate online threats, control internet usage and ensure compliance by implementing sensible web access policies.

With its 82 website categories, the BrightCloud Web Classification Service provides the granular insight customers require. Providers can use these to help their customers accurately identify websites that propagate malware, spam, spyware, adware and phishing attacks, as well as websites with sensitive content, such as adult, drugs and gambling. Using these categories and aligned groupings, organizations can achieve a more secure network, adhere to HR and compliance policies and implement and enforce effective web policies that protect users against web threats and prohibited content.

Web Reputation

BrightCloud® Web Reputation delivers an up-to-date security check of the websites users visit. This enables technology partners to add a layer of real-time security to their customers' web defenses by accurately assessing the risk posed when opening a URL, independent of its site category. This is critical as BrightCloud found that in 2020, approximately 1 in 10 malicious sites is hosted on a benign domain.[1]

While the complementary BrightCloud Web Classification Service provides site classification across 82 categories, the Web Reputation Service offers an additional lens through which a site can be evaluated as a potential threat. In addition to category, it uses site history, age, rank, location, networks, links, real-time performance, as well as other contextual and behavioral trends to determine a site's Web Reputation Index (WRI). WRI scores range from 1 to 100, with tiers split into Trustworthy, Low Risk, Moderate Risk, Suspicious and High Risk. The service also provides domain-level reputation scores based on the domain's threat history, age, popularity and other factors, such as its underlying URLs. These reputation tiers enable partners' customers to finely tune their security settings based on their risk tolerance and proactively prevent attacks by limiting the risk of end user exposure to inappropriate or malicious web content.

BrightCloud Classification Stats

- 999+ million domains and 43+ billion URLs classified
- 82 site categories, including high-risk categories
- 45+ languages
- 6 million dangerous IPs correlated with URLs

Premium Feature: Domain Safety Score

The Domain Safety Score, available as a premium feature within the Web Classification and Web Reputation Services, can help address the issue HTTPS protocols may present, in which categorization at the domain level may not reflect the actual path-level content. Network devices that do not or cannot implement SSL/TLS decryption functionality due to limited resources, cost or capabilities will be enabled to make better security filtering decisions in situations with minimal page-level visibility.

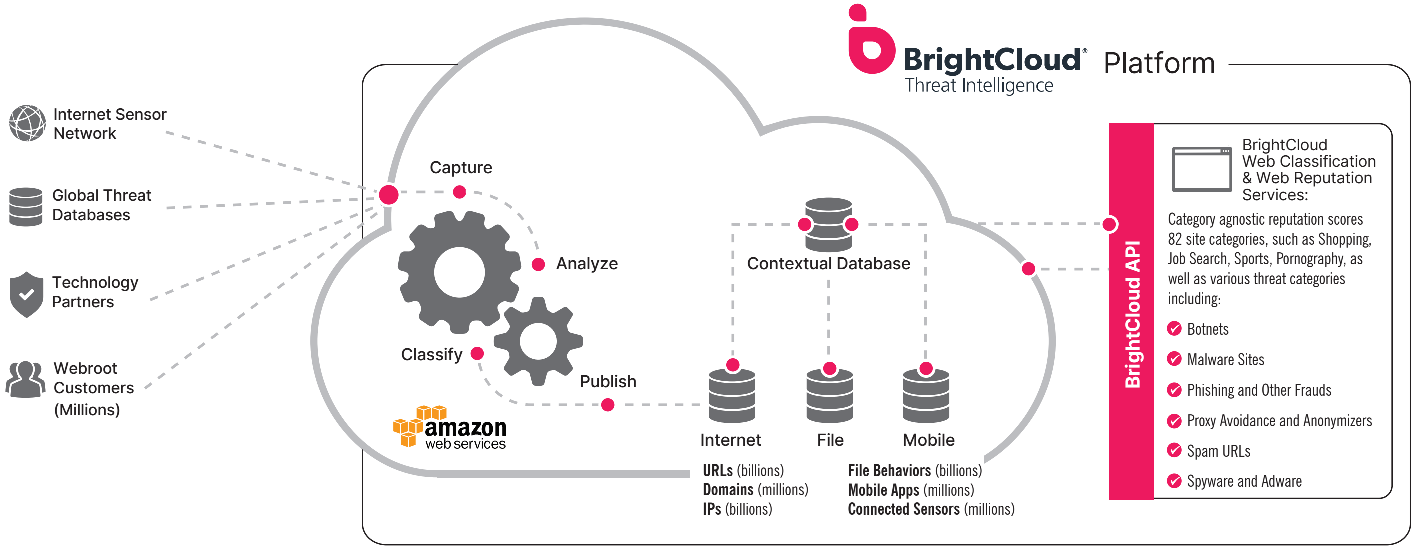
Using the Web Classification and Web Reputation Services, organizations can implement and enforce effective web policies that protect users against web threats and prohibited content, even when encrypted through HTTPS.

BrightCloud Platform

The BrightCloud® Web Classification and Web Reputation Services are powered by the BrightCloud Platform. Data on new and known sites is continuously created and refreshed, ensuring that site categorizations and reputation scores are always as current as possible.

Whenever a user visits an uncategorized site, it is dynamically crawled and scored. Each website's score is checked and adjusted over time.

As part of our ongoing efforts to enhance the BrightCloud Platform, we have introduced new threat hunting techniques, which have enabled more accurate detection and classification of malicious URLs. BrightCloud uses a proprietary and fully automated deep crawling infrastructure for threat hunting, which is combined with the BrightCloud contextual data to scan and accurately categorize thousands of URLs per second. The proactive and methodical parsing of massive quantities of network data enables the BrightCloud Platform to uncover significantly more malware URLs and to determine that, on average, 91% of the new malicious URLs discovered each day are zero-day sites. With its highly sophisticated combination of global threat sensors, machine learning algorithms and human classification, the BrightCloud Platform continuously maintains and expands its knowledge of website classifications and integrates this information for our partners.


BrightCloud® Threat Intelligence Platform
Internet Sensor Network
Global Threat Databases
Technology Partners
Webroot Customers (Millions)
Capture
Analyze
Classify
Publish
amazon web services
Contextual Database
Internet
File
Mobile
URLs (billions)
Domains (millions)
IPs (billions)
File Behaviors (billions)
Mobile Apps (millions)
Connected Sensors (millions)
BrightCloud API
BrightCloud Web Classification & Web Reputation Services:
Category agnostic reputation scores
82 site categories, such as Shopping, Job Search, Sports, Pornography, as well as various threat categories including:
✓ Botnets
✓ Malware Sites
✓ Phishing and Other Frauds
✓ Proxy Avoidance and Anonymizers
✓ Spam URLs
✓ Spyware and Adware

BrightCloud® Web Classification and Web Reputation Services

Contextualization Between Disparate Object Types

The patented, contextual BrightCloud analysis techniques enable BrightCloud to develop actionable intelligence that can predict behaviors of unknown objects. Contextualization is a "guilt by association" model that correlates the site's relationships with other scored URLs, IPs, files and mobile apps to provide a comprehensive view of the threat landscape. Mapping the relationships between these disparate data points allows BrightCloud to provide partners with highly accurate intelligence that is always up to date.

Patented contextual analysis techniques map disparate data points to provide partners with holistic intelligence beyond indicators of compromise. For example, when thousands of domains are virtually hosted on the same web server, a compromised website or faulty security configurations on that server could put the other websites at risk. Websites with the same registrant as many other high-risk websites could indicate a bad actor registering the site with malicious intent or an organization with poor security practices whose websites are prone to getting infected with malicious files, scripts or phishing pages.

The power of contextualization is to observe how known bad or known good objects relate to and communicate with other objects online. It's not just two URLs or two IPs or two apps, it's the ability to analyze associations with same and different object types, combined with more than ten years of threat history on how millions of objects have behaved over time, which results in the predictive nature of BrightCloud® Threat Intelligence Services.

BrightCloud Web Threat Insights

Threat Insights deliver additional value to BrightCloud technology partners and their customers by providing in-depth threat details that factor into the BrightCloud determination process. They offer a unique mix of information to aid security decision-making and streamline the incident response process by arming network and security operations teams with the ability to prioritize their investigations according to risk and severity.

For example, the Web Threat Insights add-on provides supplementary information on websites that host malicious or potentially unwanted files, recent threat history and the stability of the host URL's host IP(s) as possible indicators of compromise.

BrightCloud® Web Classification and Web Reputation Services in Action

Integrating BrightCloud Web Classification and Web Reputation Services into network solutions not only provides an additional layer of web filtering protection from sites that host malware or spyware, but also enables partners to offer far more granular security management. The service enhances our partners' network security solutions by increasing real-time protection against known malicious threats, unauthorized network access and Denial of Service (DoS) attacks.

These services provide insights into the types of websites being accessed. It enables partners' customers to allow users to access reputable sites, while preventing access to low reputation sites that are more likely to host malicious content, such as malware or phishing threats. In addition, Web Classification and Web Reputation Services help:

- Improve network speed by blocking unwanted and malicious content
- Power parental URL classification within a consumer internet security suite to help parents protect children against harmful and unwanted content
- Enhance or power URL filtering on next-generation firewall and IPS systems, offering greater visibility and improved control over web browsing

Partner Benefits

Differentiate yourself from your competition

1. **Enable compliance** without impacting user experience
2. **Protect with real-time** and contextual intelligence visibility based on the foundation of AI and historical threat insights
3. **Minimize the risk** by responding to evolving threats with faster speed and contextual accuracy

Leverage BrightCloud® Threat Intelligence

- Take advantage of the visibility provided through millions of sources via the world's most powerful cloud-based security analysis platform

Flexible integration options

- Simple, flexible integration options enable you to integrate the latest web classification and reputation intelligence

No impact on user experience

- Protect end users from malicious sites using real-time intelligence in a way that won't impact their online experience
- Improve network performance with granular classification categories

Partner Integration Options

Web Classification and Web Reputation Services integrate seamlessly with existing security solutions through the intuitive BrightCloud software development kit (SDK), REST services and an API. Multiple BrightCloud services can be integrated via the same SDK and may be integrated in three modes, allowing partners to select the integration and deployment type best suited to their needs:

Hosted:

- All URL queries are sent over the internet to the BrightCloud Platform.

Local Database:

- A database is downloaded locally and updated once per day.

Hybrid Model:

- A URL query first examines a locally cached database. If the URL category and WRI are not stored there, the query is then forwarded to the BrightCloud Platform for classification and scoring.

[1] 2021 Webroot BrightCloud® Threat Report

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

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.