

BrightCloud® Web Classification and Reputation Services

Real-time web threat intelligence that accurately assesses the risk a URL poses and helps enforce web policies to protect users



Overview

BrightCloud Web Classification and Reputation Services

- » The number of malicious URLs continues to grow
- » Organizations require finely tuned security to protect their users from malicious websites
- » The BrightCloud Web Classification and Reputation Services categorizes the largest URL database of its kind across 82 categories and scores website risk, regardless of internet category
- » Enables partners to develop and enhance solutions to:
 - Protect employees and improve their productivity
 - Protect the organization from legal liabilities around web usage and compliance
 - Set company usage policies

New websites emerge at astonishing rates and, with the proliferation of online threats, traditional, static, list-based internet protection services are becoming obsolete. 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 to protect themselves or their users, 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 BrightCloud® Web Classification and Reputation Services offers network and security vendors 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—over 600 million domains and 27 billion URLs to date—to generate by far the largest URL database of its kind.

Web Classification

By providing the broadest, most up-to-date, and accurate website intelligence across 82 site categories, Web Classification significantly improves visibility into all internet usage. Additionally, with the superior coverage and visibility offered by this service, partners can address their customers' key concerns which may include: employee productivity, IT and bandwidth resources, 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. Sites in the primary security risk categories that propagate malware, spam, spyware, adware, and phishing attacks are made known to all connected endpoints and services in real time. When users attempt to visit uncategorized sites, the sites are categorized dynamically using the automated Webroot classification process, which is supported by a global, multilingual team. Each Webroot URL classifier can make determinations on over 5,000 URLs per minute, resulting in coverage of over 80 million URLs per day.

In 2017, 14% of URLs were high-risk.¹

Web Reputation

BrightCloud Web Reputation delivers an up-to-date security check of the websites users visit. This enables network and security vendors 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 Webroot found that, in 2017, 14% of URLs fell into the High Risk category.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. These reputation tiers enable partner's 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

- » **600+ million** domains and **27+ billion** URLs classified
- » **82 site categories**, including high-risk categories
- » **45+ languages**
- » **8-10 million** dangerous IPs correlated with URLs

Webroot® Threat Intelligence Platform

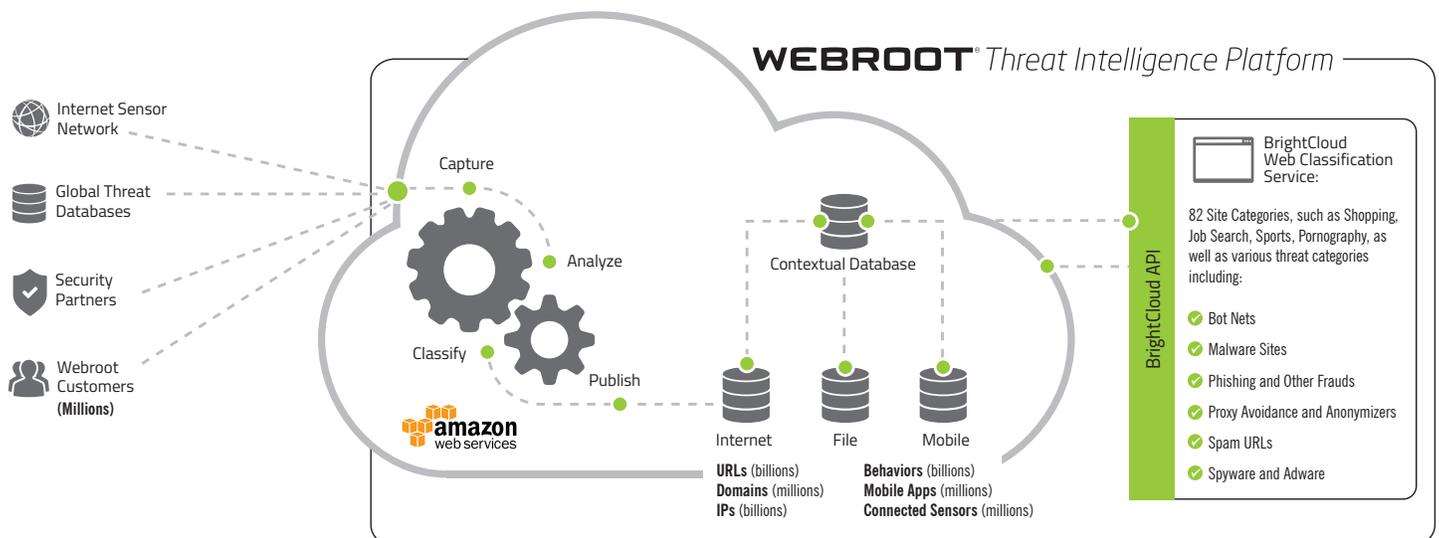
The BrightCloud Web Classification and Reputation Services are powered by the Webroot Threat Intelligence Platform. Data on new and known sites is continuously created and refreshed, ensuring that site categorizations and reputation scores are always as current as possible. Whenever a user visits an 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 Webroot Threat Intelligence Platform, we have introduced new threat hunting techniques, which have enabled more accurate detection and classification of malicious URLs. Webroot uses a proprietary, patent-pending, 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 Webroot platform to uncover significantly more malware URLs, and to determine that, on average, 75% of the new malicious URLs discovered each day are zero-day sites, not yet found by other technologies. With its highly sophisticated combination of global threat sensors, machine learning algorithms, and human classification, the Webroot Threat Intelligence Platform continuously maintains and expands its knowledge of website classifications and integrates this information for our partners.

Contextualization Between Disparate Object Types

The patented, contextual BrightCloud analysis techniques enable Webroot 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 Webroot to provide partners with highly accurate intelligence that is always up to date.

For example, a website that is well-trafficked, well-known, and associated with numerous trusted IPs is more likely to be secure, while a relatively unknown URL may present a hazard. A URL associated with a suspicious IP is likely also risky. Webroot has also recently enhanced the contextual intelligence to include common registrant information. This enables users to look up a URL and find other URLs registered by the same person or entity. Associated URLs are then grouped by reputation band from High Risk to Trustworthy.



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 Webroot BrightCloud Threat Intelligence services.

BrightCloud Web Threat Insights

Threat Insights deliver additional value to Webroot 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 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.

Partner Benefits

Differentiate yourself from your competitors

- » Offer industry-leading protection against malicious websites, using the WRI to finely tune your security settings
- » Block unwanted content to keep users safe and productive
- » Improve network performance with granular classification categories

Leverage Webroot 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

- » End users are protected from malicious sites using real-time intelligence in a way that won't impact their online experience
- » Your customers can ensure compliance through sensible access policies

BrightCloud Web Classification and Reputation Services in Action

Integrating BrightCloud Web Classification and 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.

This service provides 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 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 Integration Options.

Web Classification and Reputation Services integrate seamlessly with existing security solutions through the intuitive Webroot 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 Webroot Threat Intelligence 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 Webroot Threat Intelligence Platform for classification and scoring.

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