Webroot Security Intelligence
The World’s Most Powerful Real-Time Network Security Services
# Table of Contents

**The World’s Most Powerful Real-Time Network Security Services**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table of Contents</td>
<td>2</td>
</tr>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td><strong>Webroot BrightCloud Security Intelligence</strong></td>
<td>3</td>
</tr>
<tr>
<td>Webroot Content Classification Service</td>
<td>4</td>
</tr>
<tr>
<td>World-Leading Coverage</td>
<td>5</td>
</tr>
<tr>
<td>In Use—Webroot Content Classification Service</td>
<td>5</td>
</tr>
<tr>
<td>Webroot Web Reputation Service</td>
<td>6</td>
</tr>
<tr>
<td>In Use—Webroot Web Reputation Service</td>
<td>6</td>
</tr>
<tr>
<td>Webroot IP Reputation Service</td>
<td>7</td>
</tr>
<tr>
<td>In Use—Webroot IP Reputation Service</td>
<td>7</td>
</tr>
<tr>
<td>Webroot Real-Time AntiPhishing Service</td>
<td>8</td>
</tr>
<tr>
<td>In Use—Webroot Real-Time AntiPhishing Service</td>
<td>8</td>
</tr>
<tr>
<td><strong>In Summary</strong></td>
<td>9</td>
</tr>
<tr>
<td>About Webroot</td>
<td>9</td>
</tr>
<tr>
<td>Contact Us</td>
<td>9</td>
</tr>
</tbody>
</table>
Introduction

The Internet was once simply a place to find information. Now, people not only find each other but also carry out a large part of their personal, professional and financial lives online. Unfortunately, the growing importance of the Internet in our daily lives has spawned an arms race between those who want to exploit sensitive private data for gain and those who need to protect it from compromise.

The challenge of protecting this data has been made more difficult by a fundamental shift in the network perimeter. For many organizations, more of their sensitive data now resides outside the secure network than inside—making it imperative that security is pervasive on both endpoint and network devices.

This need for pervasive security is especially critical considering the heightened risk of an IT security breach and the huge potential damage of a breach—for organizations as well as individuals. Attackers have become both more motivated and more sophisticated. They no longer target just random Internet users, but often subject specific individuals to pinpoint social engineering scams, spear-phishing attacks, and almost undetectable zero-day exploits.

The ‘traditional’ security approach of analyzing threat information, building signature countermeasures, and then pushing out those signatures as regular updates simply cannot keep up with these new IT realities and new threats. Webroot is first security solutions provider to replace this cumbersome and outmoded approach by leveraging the cloud to protect users with collective security intelligence.

To deliver this security intelligence, Webroot built the world’s most powerful real-time threat analysis engine—the Webroot® Intelligence Network (WIN). It uses ‘Big Data’ analytics to make timely security decisions millions of times per hour. WIN also employs multiple analytic approaches—including machine learning, behavioral rules, heuristics and human analysis—to deliver the highest degree of accuracy.

This paper looks at how Webroot security intelligence network offers our Strategic Technology Partners the ability to deliver significantly superior and differentiated real-time security solutions to their customers. Webroot has harnessed the power of Software as a Service (SaaS) to deliver real-time security for network, Windows, Mac OS, Android and iOS platforms. This cloud-based solution delivers industry-leading multi-layer security protection while eliminating the impacts on performance and user experience common to conventional security solutions.

Webroot BrightCloud Security Intelligence

As a key security intelligence component of the Webroot Intelligence Network, Webroot BrightCloud™ gathers real-time intelligence about Internet web sites around the globe. To date, it has researched over 8.7 billion URLs, scored and classified over 310 million Internet domains, analyzed over 550 million IP addresses and uncovered over 9 million dangerous IPs.

The richness of real-time actionable information delivered by BrightCloud enables Webroot Partners to layer and integrate important security features into their solutions. At the same time, it eliminates cost and performance impacts resulting from having to invest heavily in cloud-based back-end systems and the datacenter infrastructure to offer such contextually aware security.
Webroot network-based security services and the real-time capabilities of the Webroot Intelligence Network are delivered through the following Webroot network security services:

- Web (URL) Content Classification Service
- Webroot Web (URL) Reputation Service
- Webroot IP Reputation Service
- Webroot Real-Time AntiPhishing Service

Security application developers can use these services to then create sophisticated security applications using intuitive Webroot software development kits (SDKs), REST services, and APIs. This makes getting Webroot security application services up and running on any platform both quick and surprisingly easy.

**Webroot Content Classification Service**

The Webroot Content Classification Service helps network and security vendors provide greater value within their enterprise security solutions. Adding the extra functionality of web content classification protects their customers against the security threats found within many website content categories. With the superior coverage—owing to the significantly improved visibility of the Internet provided by BrightCloud technology—Partners can maintain leadership in addressing key customer concerns such as:

- Boosting employee productivity
- Preserving IT and bandwidth resources
- Reducing web usage legal liabilities

Web content classification continues to create a significant number of security challenges for those trying to provide enterprises with secure web access. For starters, keeping tabs on over 629 million websites and managing a growth rate of over 47 million new web sites in the past year. While users’ exposure to phishing, keyloggers, spyware, drive-by malware and many other types of malicious code just in normal daily usage of the Internet adds a few more. Even supposedly ‘safe sites’ are now silently compromised and move rapidly between malicious and benign states to avoid detection.

The Webroot Content Classification Service provides network and security vendors with a highly effective way to ensure their enterprise customers are able to secure their users against existing and emerging web threats. It provides the broadest, most up-to-date and most accurate website classification intelligence for the creation of enforceable web policies.

1 Source: Netcraft
World-Leading Coverage
The Webroot Content Classification Service offers over 83 classification categories, providing the granular control enterprise customers demand. With over 310 million scored and classified domains, Webroot offers the most comprehensive URL coverage of any web content classification provider.

The Webroot classification and scoring system classifies over 2,500+ URLs per second at an error rate of less than 2% (versus a human error rate of 5-15%). Human classifiers then provide additional global coverage and act as a feedback loop to Webroot artificial intelligence classifications, which ensures continuous improvement.

The Webroot Content Classification Service delivers continuously updated URL information from the Webroot Intelligence Network, and its 24x7 Customer Support immediately addresses any category suggestions submitted. These contributions and others help Webroot to maintain completely up-to-date and continuously refined URL information, all of which is delivered via the Webroot Intelligence Network to its users within minutes.

In Use—Webroot Content Classification Service
• The Content Classification Service powers the URL filtering available on one of our Partner’s next-generation firewall solutions. Deployed with an on-box dataset of c.20 million URLs across all categories and augmented by cloud services to suit the traffic patterns of local user communities, it helps to increase sales and provides a popular way of administrating web activity.
• The Content Classification Service powers the URL classification data for Parental controls within a Partner’s consumer Internet Security Suite to help parents protect their children against harmful or unwanted sites.
• The Content Classification Service powers the optional URL Filtering service available on a Partner’s Next-Generation Firewall and IPS systems to offer enhanced visibility and improved control of web browsing. Integrated within their Management Center, it allows systems administrators to easily prevent access to threatening sites such as phishing sites, or improve efficiency and bandwidth usage by blocking access to unwanted web sites.

Webroot Web Reputation Service
The Webroot Web Reputation Service helps network and security vendors add a critical layer of real-time security to their customers’ web defenses by accurately observing and predicting the risk from connecting to any URL.

This additional layer of proactive protection helps defend against rapidly emerging threats by assessing a site’s risk level totally independently of its classification.

WEBROOT CONTENT CLASSIFICATION FAQs
• >310 million domains scored and classified
• 83 + categories
• 40+ languages
• >550 million IP addresses analyzed and >9 million dangerous IP’s
• Most accurate classifications
With dynamically generated user content, mashups, and the rapid rate of website deployments now so common, the structure, information and links on websites change very quickly. This speed of change provides fertile ground for malware authors. By failing to offer this layer of threat assessment other classification intelligence services leave a serious gap in protection.

The Webroot Reputation Service provides a much-needed way to reduce customers’ risks by on-the-fly scoring of the reputation levels of requested websites. These scoring metrics include site history, age, rank, location, networks, links, and other contextual and behavioral trends. The Webroot Reputation Index (see panel) ranges from 1-100 with High Risk, Suspicious, Moderate Risk, Low Risk, and Trustworthy reputation levels, enabling enterprises to finely tune security access settings and more proactively identify and prevent malicious attacks before they occur.

### Webroot Reputation Index

| 01 - 20  | High Risk | These are high risk sites. There is a high probability that the user will be exposed to malicious links or payloads. |
| 21 - 40  | Suspicious | These are suspicious sites. There is a higher than average probability that the user will be exposed to malicious links or payloads. |
| 41 - 60  | Moderate Risk | These are generally benign sites, but have exhibited some characteristics that suggest security risk. There is some probability that the user will be exposed to malicious links or payloads. |
| 61 - 80  | Low Risk | These are benign sites, and rarely exhibit characteristics that expose the user to security risks. There is a low probability that the user will be exposed to malicious links or payloads. |
| 81 - 100 | Trustworthy | These are well known sites with strong security practices, and rarely exhibit characteristics that expose the user to security risks. There is a very low probability that the user will be exposed to malicious links or payloads. |

**In Use—Webroot Web Reputation Service**

- A long-standing Webroot Partner has used the Webroot Content Classification Service to power the web filtering capabilities within its secure web gateway. They have also added the Webroot Web Reputation Service to enable policy-based management. This has enabled them to offer their customers a far stronger value proposition by allowing filtering based on the predictive scoring of the risk of visiting a website as well as the historical categorization of the website’s content.
Webroot IP Reputation Service

The Webroot IP Reputation Service extends the security intelligence capabilities of our Strategic Partners by adding dynamic IP reputation protection to their network defense solutions. To effectively stop the ever-increasing volume of network based IP threats that attack enterprises networks, Webroot provides Partners with a constantly updated feed of ‘known malicious’ IP addresses.

Rather than relying on static (and quickly out of date) publicly available Black Lists, the Webroot IP Reputation Service enables our Partners to integrate a continuously updated feed (every 5 minutes) into their network devices of all of our dynamically generated IP Reputation findings.

The near real-time intelligence of the Webroot IP Reputation Service is driven by a sophisticated sensor network that identifies key IP threat types, including: Spam Sources, BotNets, Windows Exploits, BotNets, Scanners, and more (see diagram).

As with all Webroot cloud-driven network security services, the Webroot IP Reputation Service offers a major secondary benefit: It avoids the taxing security processing overheads that other IP Reputation services impose, while greatly enhancing Webroot Partner customers’ ability to counter IP-based threats.

The benefits of stopping ‘known bad’ traffic at the network’s edge are clear. Among these is a dramatic improvement in security efficacy through the reduction in time required to discover for malicious IPs. The ease with which IP threats are now identified and stopped also provides significant processing efficiencies.

Use Cases — Webroot IP Reputation Service

- The Webroot IP reputation data powers a Partner’s new cloud-based IP Intelligence service that detects and stops IP addresses associated with malicious activities from accessing their customers’ networks.
- Another Partner uses the Webroot IP Reputation service to provide its network security products with increased real-time protection against known malicious threats, unauthorized network access and Denial of Service (DoS) attacks. They have also combined all of the Webroot Security Intelligence services to create the security industry’s most comprehensive real-time solution that stops attacks even as their launch sources are changing!
Webroot Real-Time AntiPhishing Service

The Webroot Real-Time AntiPhishing Service uses new proprietary technology within the Webroot Intelligence Network to protect a Partner’s web users by ensuring they are always connected to a legitimate website.

In a recent survey of IT Directors—conducted by Webroot in the USA and the UK—we found the number-one Internet security breach reported by over 55% of respondents during 2012 was a phishing attack. Phishing and spear phishing have grown in popularity to become the most common attack vector. With a little online research hackers can often find and use data to fool a recipient into submitting to an illegitimate request for their information. By playing on users’ trust and using a little social engineering, attackers can easily trick even sophisticated users into engaging in activity that leads to hijacking their data or identity.

Phishing also reflects how easy it is to create a ‘clone’ of a legitimate website. The user will be totally unaware they are being spoofed. These attacks work by obfuscating URLs and directing traffic to counterfeit websites that attempt to trick users into divulging sensitive information. This is bad news if the user is conducting on-line banking, connecting to a sensitive system, or carrying out any other type of sensitive transaction. Phishing now represents a very real and significant threat to anyone transacting business on the Internet.

In extensive testing Webroot’s new, highly-automated machine learning approach is detecting phishing sites three to five days ahead of competitors’ antiphishing technology. This represents a major antiphishing breakthrough. Early detection of these sites is essential as they ‘live’ for such a short period of time, and are quickly taken down to avoid detection.

The Webroot Real-Time Antiphishing Service works by evaluating any URLs requested by a user and scoring them ‘on-the-fly’ for any phishing risks based upon hundreds of “features” on the site. Features scored include the content on the page, reputation information of the domain, and numerous other factors. Machine learning determines which features are significant for each scanned URL and what weighting to apply to each in the classification. It is also capable of feeding-back human evaluations into the machine model to continually increase the accuracy of the determinations.

The new Webroot Real-Time AntiPhishing Service is available now as the latest Webroot security service for our Strategic Partners network solutions.

Use Case—Webroot Real-Time AntiPhishing Service

- Webroot has added Real-time AntiPhishing Protection to the Webroot Secure Web Gateway SaaS offering to further protect enterprises from phishing attacks, which are a primary vector for Advanced Persistent Threats.

- A major anti-fraud service that protects over 5,000 enterprises from phishing and other frauds now uses the Webroot Real-Time AntiPhishing Service. The company found that its existing combination of some light automation and manual review of URLs was simply not able to keep up with the high volumes of phishing URLs encountered. Whereas Webroot machine learning technology to process URLs for phishing eliminated most of manual review and confined it to phishing highly likely and high-value targets.
In Summary

Webroot is now recognized as a major innovator in the IT Security Industry. Recent awards like the 2012 Edison Award for Innovation (the first ever for an IT Security vendor) and Frost & Sullivan’s 2012 North American Frost & Sullivan Product Differentiation Excellence Award and many others bear witness to this.

Webroot technologies are built on a foundation of robust security intelligence and the application of ‘Big Data’ analytics to make highly accurate security decisions, millions of times per hour.

These foundations enable Webroot to offer the world’s most accurate and powerful real-time security technologies. These solutions help our Strategic Partners stay ahead of the curve in their network security offerings, and simplify the enhancements they provide by making it easy to integrate Webroot real-time security intelligence offerings into their own.

About Webroot

Webroot is bringing the power of software-as-a-service (SaaS) to Internet security with its suite of Webroot SecureAnywhere™ offerings for consumers and businesses, as well as offering its security intelligence solutions to organizations that also focus on cyber-security, such as Palo Alto Networks, F5 Networks, Corero, Juniper, and others.

Founded in 1997 and headquartered in Broomfield Colorado, Webroot is the largest privately held Internet security organization based in the United States.


Contact Us

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

Webroot Headquarters—USA
385 Interlocken Crescent
Suite 800
Broomfield, Colorado 80021
USA
Tel: +1 800 870 8102

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

©2013 Webroot Inc. All rights reserved. Webroot is the registered trademark of Webroot Inc. in the United States and/or other countries. All other trademarks are properties of their respective owners.