WEBROOT
an opentext company

BrightCloud® File Reputation Service

Dynamic file reputation intelligence to stop malware distribution

Overview

- As malware continues to proliferate, organizations of all sizes need additional layers of defense within their security infrastructure
- Network-based malware detection technologies can be overwhelmed and bypassed
- File intelligence can quickly identify malware and trustworthy files so potential threats can be investigated

Malware hides within the sheer volume of files encountered by companies every day. The AV-TEST Institute registers over 350,000 new malicious programs every day. This volume of malware makes the need for strong file reputation capabilities critical in combating threats, as well as freeing up valued security resources by allowing known good files to bypass sometimes over-taxed security infrastructure.

The BrightCloud® File Reputation service provides up-to-the minute file intelligence derived from millions of real-world sensors. Each file is analyzed by the latest machine learning techniques and vetted through years of threat expertise. This real-time lookup service of known malicious and whitelisted file identifiers helps to effectively stop the distribution of threats through networks. This verification significantly reduces the amount of 'noise' by enabling policies to automatically determine which files to allow, block, or investigate further, allowing security administrators to focus on unknown potential threats.

This service uses industry standard file hashes as fingerprints to uniquely identify files, regardless of filename, platform, encryption or password protection. It responds to authorized requests to look up the reputation of the file hash in the Webroot® Platform.

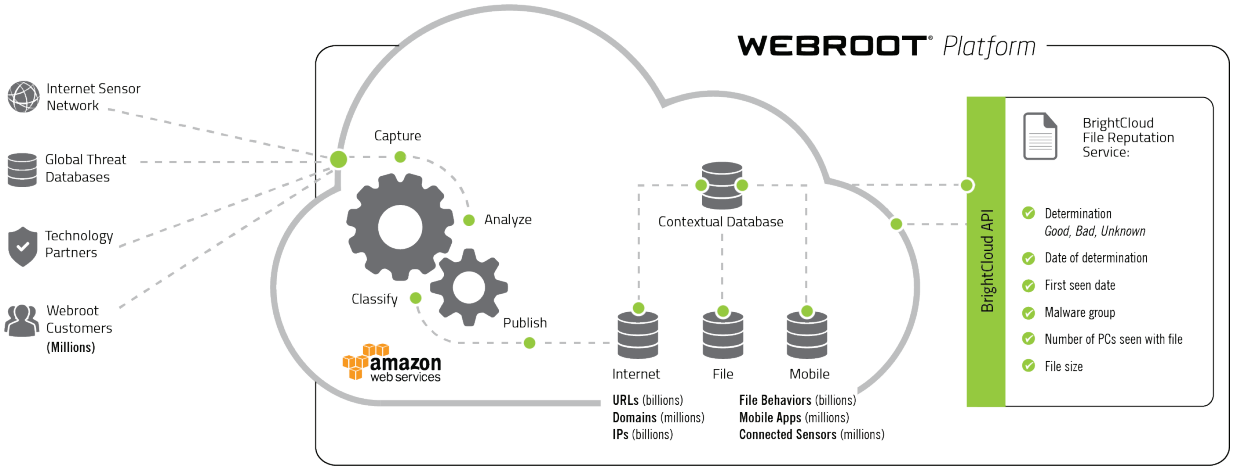
The service then responds with a determination of Good, Bad, or Unknown/Unclassified, as well as several other security attributes associated with the file, including:

- The type of malware it contains
- The number of times the file has been seen across the Webroot Platform
- When it was first detected
- The date of its classification or most recent determination

The Webroot Platform is updated via millions of enterprise and consumer endpoints and network security devices around the globe, continuously receiving the latest information on emerging threats. In addition, file data is correlated with URLs, IPs, and mobile apps to provide a comprehensive view across the threat landscape. Mapping the relationships between these different data points enables Webroot to provide partners with highly accurate intelligence that is always up to date. This automated network dramatically reduces the time to detect for emerging threats and provides real-time protection to prevent malicious files from entering networks and spreading to unsuspecting users. To date, Webroot BrightCloud Threat Intelligence contains more than 36 billion detailed file behavior records and grows more intelligent by the day.

93.6% of malware in 2019 was only seen on a single endpoint.[1]

[1] Webroot Inc. "2020 Webroot Threat Report." (February 2020)



Webroot BrightCloud® File Reputation Service

Partner Benefits

» **Differentiate yourself from your competition**
Reduce noise at the network edge, freeing up your customers' security resources to focus on the most pressing threats

» **Leverage the Webroot® Platform**
Harness collective threat intelligence from millions of sources via the world's most powerful cloud security platform

» **Easy to integrate, easy to use**
Simple integration through RESTful API and an SDK into your solution

» **No impact on your network**
Protects through your network devices and increases user capacity by eliminating unwanted traffic

The BrightCloud File Reputation Service in Action

The BrightCloud® File Reputation Service helps network edge appliances, such as next-generation firewalls and intrusion detection/prevention devices, determine whether files are trustworthy, malicious, or require further investigation. Additionally, it helps cloud-based storage providers ensure customers' stored files are malware-free, and enables web and email hosting providers to scan hosted files to ensure that both the website/email owner and provider are aware of any hosted or queued malware.

File Reputation data is backed by more than 17 million real-world endpoints and their encounters with everyday applications, including malware. Because of the constantly updated feed, the File Reputation Service is often much faster than other leading services in discovering zero-day threats.

Additionally, when coupled with BrightCloud® Streaming Malware Detection, the File Reputation service makes an especially effective tool against traditional and modern malware.

Designed to combat the challenges of polymorphic malware, BrightCloud Streaming Malware Detection allows our partners' devices to make determinations at the network level enabling users to quickly allow, block, or flag files for investigations. Since the files often don't need to be fully downloaded, this service frees up network bandwidth by dropping malware at the perimeter and eliminates the need to re-inspect benign files.

Easy Integration

Traditional antivirus solutions offer a heavy and rigid approach to integration, sacrificing usability and performance for companies trying to integrate them. The BrightCloud File Reputation Service provides an easy to integrate API so partners can use the extensive Webroot database to build malware detection into products and better protect users. Additionally, this service combines with existing security solutions through the same SDK as other BrightCloud services, making integration as simple and straightforward as possible.

About Webroot

Webroot, an OpenText company, harnesses the cloud and artificial intelligence to protect businesses and individuals against cyber threats. We provide endpoint protection, network protection, and security awareness training solutions purpose built for managed service providers and small businesses. Webroot BrightCloud® Threat Intelligence Services are used by market leading companies like Cisco, F5 Networks, Citrix, Aruba, A10 Networks, and more. Leveraging the power of machine learning to protect millions of businesses and individuals, Webroot secures the connected world. Webroot operates globally across North America, Europe, Australia 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