WEBROOT®
Smarter Cybersecurity™

BrightCloud® File Reputation Service

Integrate up-to-the-minute file intelligence so your customers can focus resources on pressing threats

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

The AV-TEST Institute registers over 350,000 new malicious programs every day, and the growth in malware continues to expand at an alarming rate. Nearly all malware delivery uses polymorphism—either at the server level, where every infection generated is a unique variant, or the threat itself is polymorphic, making it unique to the recipient. In 2018, 93% of malware seen was polymorphic.[1] This tactic poses a major problem to traditional security approaches, which struggle to discover singular variants. That's why the Webroot threat intelligence and discovery model was specifically designed to detect and prevent unique polymorphic infections.

The BrightCloud® File Reputation Service provides technology partners up-to-the minute file intelligence derived from millions of real-world sensors and analyzed by the latest machine learning techniques. This continuously updated real-time lookup service of known malicious and whitelisted file identifiers allows partner solutions to effectively stop the distribution of emerging threats through their customers' networks, so security administrators can focus their limited resources on the unknown potential threats. This real-time verification significantly reduces the amount of 'noise' by enabling policies to automatically determine which files to allow, block, or investigate further.

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

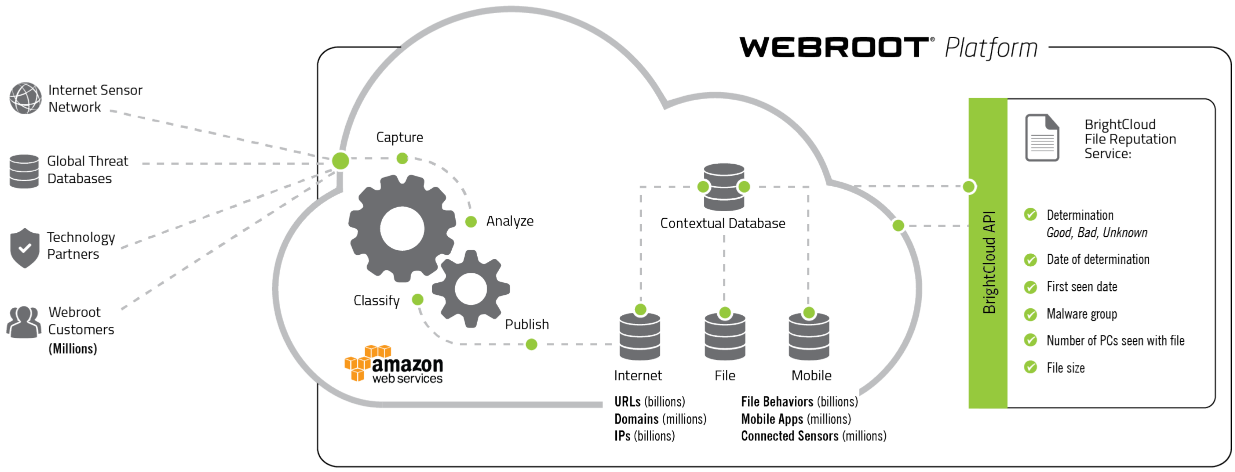
» When it was first detected

» 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 Threat Intelligence contains more than 31 billion detailed file behavior records and grows more intelligent by the day.

93% of malware in 2018 was only seen on a single endpoint.[1]

[1] Webroot Inc. "2019 Webroot Threat Report." (Feb 2019)



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.

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 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

DS _ 022819 _ A4