BrightCloud® File Reputation Service

OVERVIEW

- As malware continues to proliferate, corporations of all sizes need additional layers of defense within their security infrastructure
- Traditional cybersecurity can't keep up with the volume and speed of modern malware
- Dynamic file intelligence is required to effectively stop the distribution of emerging malware

The AV-TEST Institute registers over 390,000 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 fact, Webroot® has found that over 97% of malware is only seen on a single endpoint. 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 extends next-generation Webroot® threat intelligence by offering partners a dynamic, up-to-the-minute file reputation service to protect their customers. This continuously updated real-time lookup service of known malicious and whitelisted file identifiers allows IT Security administrators to easily and effectively stop the distribution of emerging threats through their networks, before they infect devices. In addition to basic file determinations, administrators can access rich data around the latest threats that have not yet been classified.

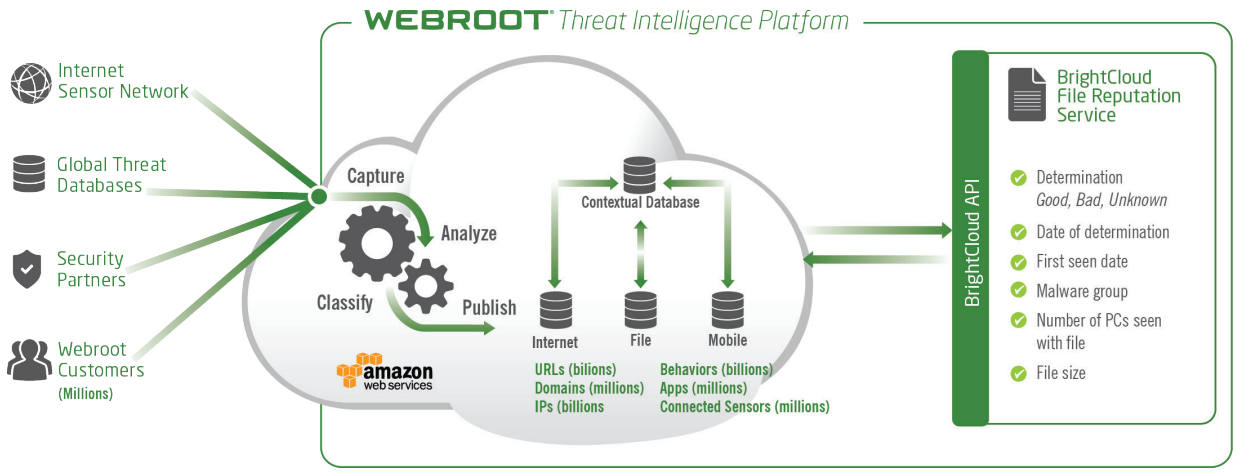
This service uses industry standard MD5 file hashes as fingerprints to uniquely identify files of all types, regardless of filename, platform, encryption or password protection. It responds to authorized requests to look up the reputation of the MD5 file hash in the Webroot® Threat Intelligence Platform. 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 BrightCloud Threat Intelligence Services
- When it was first detected
- The date of its classification or most recent determination

BRIGHTCLOUD® FILE REPUTATION SERVICE

The Webroot Threat Intelligence 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 over 9 million detailed file behavior records and grows more intelligent by the day. The File Reputation Service handles over 4 billion queries a day, equating to 50,000 per second.

BrightCloud® File Reputation Service



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.

PARTNER BENEFITS

- **Differentiate yourself from your competition**
  Protect your customers from malware at the network edge, before it reaches end users
- **Leverage the Webroot® Threat Intelligence 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 safe before they are delivered to an end user. 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.

With zero-day malware breakouts like Regin and the CryptoLocker family, the BrightCloud File Reputation Service was able to identify or capture 30% more files infected with these malware than some of most popular engines could even detect on day zero. Lab simulations showed that it took some of the most popular virus engines up to 30 days from the time it was first seen to mark it as malware.

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 MD5 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.

The BrightCloud File Reputation Service can also be supplemented by the BrightCloud Threat Investigator. This service provides additional data on the primary URLs, IPs, files, and mobile apps which impact the score of the IP address being researched, to better understand why a score was given and proactively protect against associated malicious actors.

About Webroot

Webroot delivers next-generation endpoint security and threat intelligence services to protect businesses and individuals around the globe. Our smarter approach harnesses the power of cloud-based collective threat intelligence derived from millions of real-world devices to stop threats in real time and help secure the connected world. Our award-winning SecureAnywhere® endpoint solutions and BrightCloud® Threat Intelligence Services protect tens of millions of devices across businesses, home users, and the Internet of Things. Trusted and integrated by market-leading companies, including Cisco, F5 Networks, Aruba, Palo Alto Networks, A10 Networks, and more, Webroot is headquartered in Colorado and 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