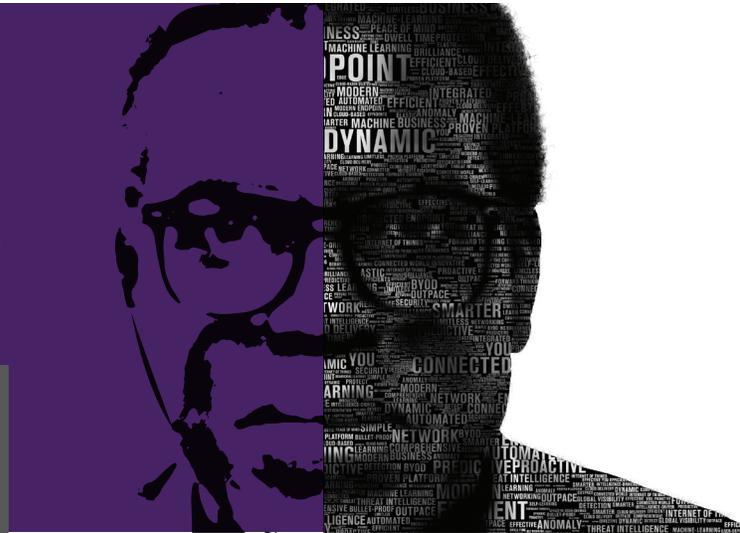


# BrightCloud® Mobile App Reputation Service

Quickly and accurately determine which apps are safe for your customers



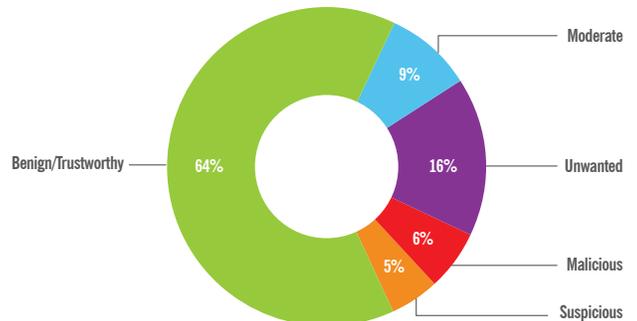
## Overview

- » Due to rising popularity and Bring Your Own Device (BYOD), malware is increasingly distributed through mobile apps
- » Mobile Device Management (MDM) vendors, mobile carriers, application distributors and other providers need to ensure customers' mobile endpoints are protected
- » Webroot offers providers a way to protect their customers and differentiate their solutions through:
  - Nearly 50M Android® and iOS® apps analyzed, and growing each day
  - Advanced protection against mobile malware and Potentially Unwanted Applications (PUAs), powered by the Webroot® Threat Intelligence Platform

The exploding popularity of smartphones and tablets has created a major new threat vector: the mobile application. With the large volume of apps now available, cybercriminals can easily disguise and distribute malicious code to unsuspecting victims. In fact, apps have become the primary vehicle to distribute mobile malware, and the exponential growth of apps is only compounding the problem. Since 2012, Webroot has found that the percentage of trustworthy/benign mobile apps has dropped from 64% to 21% in 2016.<sup>1</sup> How can MDM vendors, mobile carriers, and application distributors quickly and accurately determine which apps are safe to make available to their customers?

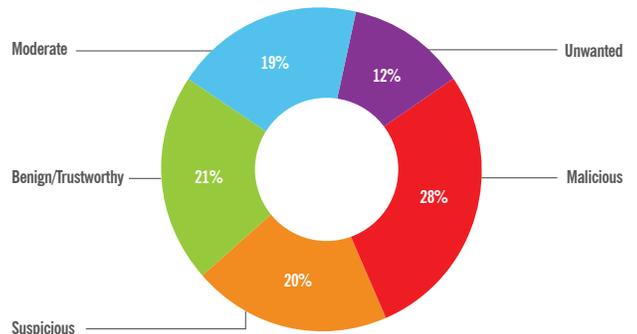
The BrightCloud® Mobile App Reputation Service helps vendors who provide mobile management and security solutions address the new security vulnerabilities that mobility creates. Powered by the Webroot® Threat Intelligence Platform, the service continuously analyzes applications from app stores and other online sources, identifying threats and allowing IT security professionals to restrict access to applications based on individual policies and risk tolerance using a six-tiered

Nearly 2 Million Android Apps Classified



2012 Android Scan Results

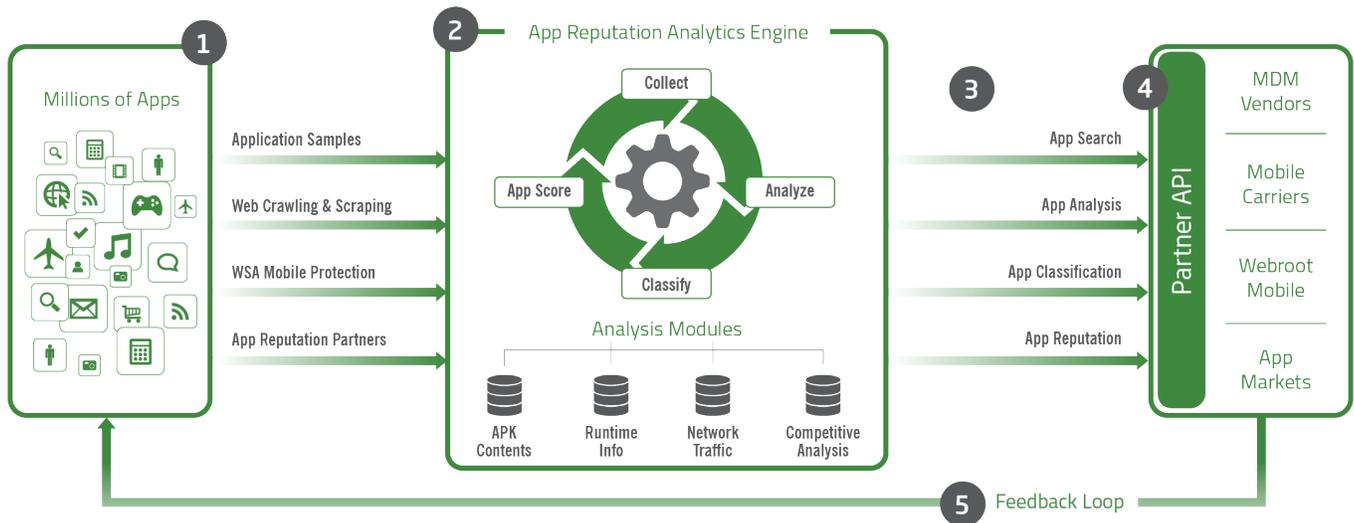
Nearly 50 Million Android Apps Classified



2016 Android Scan Results

*Since 2012, Webroot has found that the percentage of trustworthy/benign mobile apps has dropped from 64% to 21% in 2016.<sup>1</sup>*

<sup>1</sup> Reputable app stores are a reliable source for mobile apps. Webroot actively searches sources where malicious apps are likely to be found, resulting in a higher percentage of those being uncovered.



**BrightCloud® Mobile App Reputation Service**

scoring model. Webroot partners can now integrate one of the most powerful app reputation services on the market, leveraging intelligence on nearly 50 million new and updated mobile apps, and counting, to deliver safe and compliant applications.

**Partner Benefits**

- » **Differentiate yourself from your competition**  
Offer your customers industry-leading protection against known, newly-released and unknown mobile malware
- » **Leverage the Webroot® Threat Intelligence Platform**  
Harness collective threat intelligence from millions of sources via the world's most powerful cloud security network
- » **Easy to integrate, easy to use**  
Simple integration has the flexibility to create and enforce policies based on app band classifications
- » **No impact on user experience**  
Manage daily blacklist updates and real-time app lookups through a centralized management console without disrupting user experience

**How the BrightCloud Mobile App Reputation Service Works**

The figure below presents a process flow showing how this service collects, analyzes and distributes app data to partners and customers.

**1. Collection**

The service collects millions of apps from app markets, third party sites, app sharing services, strategic partners, and Webroot SecureAnywhere® Business Mobile Protection users.

**2. Analysis**

After the apps are fed into the App Reputation Analytics Engine, an automated, multi-staged analysis process collects detailed data on each one.

**3. Classification and Scoring**

Each app is categorized and assigned a score based on detailed data analysis, using heuristics and machine learning advanced algorithms. This approach allows for granular detail on what the app actually does once installed, enabling the BrightCloud service to categorize apps ranging from trustworthy to malicious.

**4. Partner API**

The classification and scoring results allow Webroot partners to analyze apps or app data via a web service API.

**5. Continuous Feedback**

New and updated apps are fed back into the system for the most up-to-date intelligence possible.

Webroot categorizes and scores mobile apps based on characteristics and behavior to help vendors enforce reputation-based policies that reduce the risk of customers installing malicious or unwanted apps.

## The BrightCloud Mobile App Reputation Service in Action

Webroot has streamlined the process of analysis to provide concise classification and other information on mobile apps in the database. A simple band classification enables Webroot partners to implement effective mobile app usage policies. This is the main advantage of this service: allowing or blocking mobile apps based on the policy designed to safeguard the unique interests of business and its users. It provides flexibility for MDMs, mobile carriers and app market providers to decide how to use the app information and adapt it for specific management requirements. With millions of mobile applications available and new apps introduced every day, Webroot partners are assured that their customers are protected.

### App reputation is classified as:

- ① Malicious
- ② Unwanted (PUA)
- ③ Suspicious
- ④ Moderate
- ⑤ Benign
- ⑥ Trustworthy

## Flexible Integration Options

Partners can easily integrate BrightCloud® Threat Intelligence Services into their own solutions using the intuitive Webroot® software development kit (SDK), REST services, and API. The BrightCloud Mobile App Reputation Service integrates with existing security solutions through the same SDK as other BrightCloud services, simplifying integration of multiple services. Depending on the business need, BrightCloud Threat Intelligence Services may be integrated in different modes, enabling partners to select the integration and deployment type best suited to their needs. The options are:

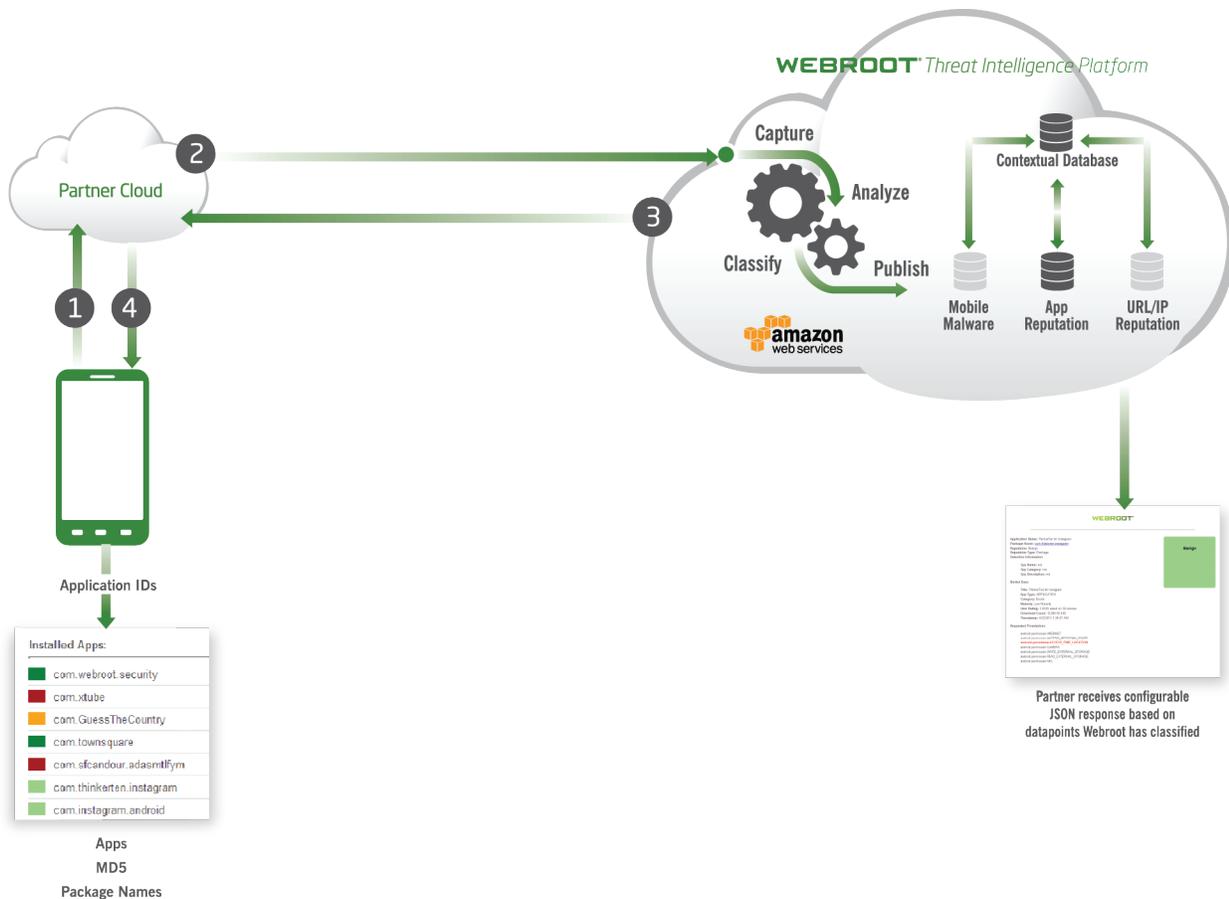
### » Hosted

All app reputation requests are sent over the internet to the Webroot Threat Intelligence Platform

### » Hybrid Model

An app reputation query can first examine a partner developed, locally cached database. If the app reputation is not stored there, then the query can be forwarded to the Webroot Threat Intelligence Platform for classification

### Mobile App Reputation Sample Integration



The BrightCloud Mobile App 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 an application's score for better insight into why a score was given and proactive protection against associated malicious actors.

Strategic partners across the globe have had tremendous success integrating Webroot into their network solutions, from MDM providers to mobile carriers. Because Webroot provides an uncomplicated integration, this solution can be implemented simply and easily by mobile vendors worldwide.

#### About Webroot

Webroot delivers next-generation network and 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 millions of devices across businesses, home users, and the Internet of Things. Trusted and integrated by market-leading companies, including Cisco, Citrix, 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](http://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