Mobile App Reputation Services

Understanding the role of App Reputation Services in delivering “Enterprise Grade” Mobile Security

A Whitepaper by The Radicati Group, Inc.
# Table of Contents

Introduction........................................................................................................................................3
1.0 The Growth in Number of Mobile Apps.....................................................................................4
2.0 Different Layers of Mobile Security............................................................................................4
3.0 Current Approaches for Dealing with App Security...................................................................5
4.0 The Webroot® App Reputation Service.....................................................................................7
5.0 Conclusions and Recommendations...........................................................................................11

*This whitepaper was sponsored by [Webroot](https://www.webroot.com)*
INTRODUCTION

Smartphones and tablets continue to be heavily adopted by enterprises and consumers alike and have changed the way people live and work. While this leads to greater user freedom and empowerment, it also opens the way to more security vulnerabilities than ever before, as mobile devices are increasingly targeted by hackers and cybercriminals.

Although security concerns exist at all levels of the mobile ecosystem—including mobile device hardware, the operating system layer, and the mobile browser capabilities—nowhere is the threat of malware and malicious activity more challenging than at the application level. The sheer number of available apps and their various sources presents an enormous threat vector for malware, particularly as users are not always aware of the threats those apps can pose.

While some of the billions of apps available via mobile app stores have undergone approval testing, others are only minimally vetted before being accepted for store distribution. The Apple App Store boasts 775,000 apps as of January 2013, and Google Play had 900,000 apps online as of May 2013. Apple has become famous for its rigorous approval process, but Google has taken a more relaxed stance, allowing app developers greater freedom to upload to the Play store.

Regardless of the amount of testing that an app vendor may impose, the sheer volume of these apps makes it impossible for users and organizations to be certain which apps are trustworthy. In addition, app behavior can range widely from mildly annoying pop-ups, to unwanted overuse of device communication capabilities, to outright downloading of malicious code.

The only way to successfully address the onslaught of apps and the risks they can represent is to utilize a mobile app reputation service. Mobile app reputation services can provide intelligence and granular threat assessments on millions of apps and are an essential aspect of a complete security strategy for mobile app developers, Mobile Device Management (MDM) vendors, mobile app vendors, mobile carriers, and anyone who needs to deliver application security to their customers.

This whitepaper discusses the need for mobile app reputation assessment, and presents the Webroot® App Reputation Service and the unique threat protection capabilities it offers to ensure that mobile applications are safe and compliant. In addition, the Webroot App Reputation Service provides a wealth of general information about app characteristics which can be used to set policies on app delivery and behavior permissions.
1.0 THE GROWTH IN NUMBER OF MOBILE APPS

The number of apps available for mobile devices continues to climb sharply. In early 2013, Apple reported App Store additions at an approximate rate of 20,000 per month, and Android apps were appearing at a similar pace. The publication process for apps is relatively simple, increasing not only the number of apps, but the likelihood of risk associated with each one.

As of mid-2013, there had been approximately 100 billion app downloads, as Google announced its 48 billionth app download and Apple announced its 50 billionth a day later. Based on these trends, we anticipate an additional 100 billion app downloads within the next year.

2.0 DIFFERENT LAYERS OF MOBILE SECURITY

The drastic increase in the number of apps available is fueled in large part by the growing number of mobile devices in use. The Bring Your Own Device (BYOD) trend has become popular across all verticals. While many organizations felt uneasy, initially, about employees carrying corporate data on devices that could so easily be misplaced or stolen, BYOD is rapidly becoming the norm. As more and more mobile devices continue to access and carry sensitive work-related information, mobile security is more important than ever.

Today, we can think of mobile security as three different layers:

- **The device layer** protects and enforces policies on the physical hardware of a mobile device. Most mobile devices today come with cameras, GPS, Bluetooth, and other sophisticated hardware that can be exploited by cybercriminals. Securing these device-level features lays the foundation for enforcing security on the operating system and application layers, which rely on device-level features for input.

- **The operating system layer** is the driving force of a mobile device, taking input from the user and providing feedback in return. This layer is fundamental to device security, as it enforces passcodes for device access, executes remote wipe features, and blocks access to device communication resources, such as GPS and Bluetooth connectivity. However, protection at this layer is unable to recognize unwanted or malicious behavior by individual apps.
• *The app layer* is where security must address loss of data. Applications can store sensitive data that users need to access on a daily basis. In order to ensure the integrity of the data contained within apps, organizations use additional forms of authentication, e.g., encryption, VPN tunneling, etc. Furthermore, certain apps cannot be trusted, such as games or rogue mobile banking apps, and must be blacklisted based on their impact to user productivity, data exploitation, and other malicious or undesirable activity.

Table 1 summarizes some of the security threats that may be found at each layer.

<table>
<thead>
<tr>
<th>Mobile Security Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Layer</strong></td>
</tr>
<tr>
<td>Device</td>
</tr>
<tr>
<td>Operating System</td>
</tr>
<tr>
<td>Applications</td>
</tr>
</tbody>
</table>

**Table 1: Common Security Threats at Each Layer of a Mobile Device**

### 3.0 CURRENT APPROACHES FOR DEALING WITH APP SECURITY

The security elements for the device and operating system layers have remained manageable for MDM vendors. The apps, however, are difficult to manage, since they can be updated on a daily basis. This makes ensuring security at the application layer a very difficult proposition. Today, app security is normally addressed with some of the following techniques:

• *Mobile device management* is seen as the base level of security that utilizes device and operating system controls to keep devices secure. While this type of security can keep a device as a whole secure, the features available for applying granular protection to individual apps are very limited.
- **App whitelisting/blacklisting** addresses the security of applications on a mobile device. Administrators decide which apps to block or allow in a binary fashion. While this approach can address the problem of app security, the success of this approach is directly proportional to the number of man-hours an administrator spends examining and categorizing apps. With the rising volume of apps available, it is impossible for static whitelist/blacklists to remain current. In addition, methods of this type generate false positives all too easily.

- **Containerization** also addresses application security, but is a time-consuming process that should be reserved for custom-built apps or apps that contain extremely sensitive data. Although it is not necessary to containerize apps that are relatively harmless, these apps must be addressed with some type of security feature. Containerizing every app would be too labor intensive.

Table 2 summarizes these approaches to mobile device protection and some of the limitations they present with regard to app security.

<table>
<thead>
<tr>
<th>Protecting Mobile Devices</th>
<th>Approach</th>
<th>Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile Device Management</td>
<td>Focused mainly on device-level controls and not at app-borne threats.</td>
<td></td>
</tr>
<tr>
<td>App Whitelisting /</td>
<td>Binary approach that is too labor-intensive for the millions of apps</td>
<td></td>
</tr>
<tr>
<td>Blacklisting</td>
<td>available. Can easily generate false positives.</td>
<td></td>
</tr>
<tr>
<td>Containerization</td>
<td>Only necessary for enterprise apps, not well-suited for personal or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&quot;mass-market&quot; apps. Malicious apps can still infect the device layer even</td>
<td></td>
</tr>
<tr>
<td></td>
<td>if they are containerized.</td>
<td></td>
</tr>
</tbody>
</table>

Table 2: Protecting Mobile Devices

In the current mobile landscape, there are simply too many apps to handle with containerization or whitelisting/blacklisting. Furthermore, a whitelisted app can easily turn malicious with an update. While it is certainly true that some apps, such as enterprise-specific apps, must be containerized or treated with special care, the majority of apps should be secured through an automated process that offers granularity about an app’s behavior.
App reputation services use a large number of inputs to automatically evaluate mobile apps, including malware signatures, URLs, and much more. Using this broad range of inputs, an app reputation service can go beyond binary ranking systems. In addition, with the large amount of inputs used, an app reputation system can generate reputation scores that result in few, if any, false positives.

4.0 THE WEBROOT APP REPUTATION SERVICE

While the protection of corporate-sanctioned apps is achieved via intricate, personalized methods such as containerization and app wrapping, protection from the millions of non-corporate-sanctioned apps is too restrictive when addressed solely with whitelists/blacklists. On the other hand, this protection cannot be left entirely unregulated. Many times, mobile device users trust apps with their information simply because they are downloaded from Google Play or the Apple App Store. IT administrators need the flexibility to set controls on mobile applications based on variable criteria.

To address this issue, the Webroot App Reputation Service gauges the risk factor of an app using a massive threat intelligence database, giving partners and customers the ability to manage the delivery of mobile applications that are safe and compliant.

The service functions as follows:

- **Collection** – the App Reputation Service collects millions of applications from app markets, third-party sites, app sharing services, strategic partners, and Webroot SecureAnywhere® Business Mobile Protection users.
- **Analysis** – after the applications are fed into the App Reputation analytics engine, an automated, multi-stage analysis process collates detailed data on each application.
- **Classification and Scoring** – each app is categorized and assigned a score based on algorithms using detailed analysis data. This approach allows for granular detail on what the app actually does once installed, enabling Webroot to better determine if an app is trustworthy, neutral, malicious, or suspicious. Classification criteria extend beyond simply recognizing whether an app contains some form of malware designed to exploit the device or its operating system. Attributes such as unnecessary ads, overly chatty pop-ups, dubious privacy policies and access requests, and many other forms of invasive or unwanted behaviors are analyzed.
• *Partner API* – the Classification and Scoring results allow Webroot partners to analyze apps and app data via a web service API.

• *Feedback Loop* – information collected by Webroot partners is then gathered and looped back into the App Reputation analytics engine. Using the data and analysis results provided by the Webroot App Reputation Service, MDM vendors, mobile carriers, app developers and application marketplaces can develop solutions that incorporate app reputation to ensure their customers are protected from malicious or unwanted mobile apps.

To determine the score for each app, the Webroot App Reputation Service uses security information from the Webroot® Intelligence Network (WIN), which collects billions of pieces of information from multiple sources, including data from customers, test laboratories, and intelligence shared between security vendors. Using WIN, the Webroot App Reputation Service is differentiated by its ability to leverage automated machine learning to collect, analyze, and classify millions of mobile applications. The service also uses proprietary heuristics that scan apps to perform behavioral assessment.

Figure 1 shows how the Webroot App Reputation Service arrives at a trust level for an app and its ability to deliver this data to its partners.
Webroot has streamlined the process so that concise app reputation classification and other useful app data is transparent to administrators. Using a RESTful web service API, Webroot allows MDM and other applications that manage mobile app usage policies to view the information collected. Applications can be checked by several lookup mechanisms, including package name and MD5 hash. Ranging from Malicious to Trustworthy, this simple banding classification system provides an easy-to-implement solution for Webroot partners. The API is designed to be flexible, so developers can set permissions based on numerous data points, not just banding classification, to determine application policy compliance.

Data elements exposed through the API include:

- Application reputation
- Blacklist
- Whitelist
- Basic file and package information
- Digital certificate information
- Manifest data
- Permission requests
- Requested phone features

Figure 1: Webroot App Reputation Service Process
Earlier this year, 2.62 million Android apps and 670,000 iOS apps were analyzed using Webroot’s app reputation ratings. The results of this analysis are shown in Figure 2 below.

This snapshot of the rankings taken from the Webroot App Reputation Service is quite alarming; more than 4 out of 10 Android apps contain some form of malware, dubious permissions, or other cause for suspicion. iOS apps were shown to be less dangerous on the whole, due to Apple’s strict app vetting process, but even these apps can have unwanted characteristics.

The Webroot App Reputation Service lets administrators restrict apps based on reputation score, but it also allows for individual app permissions. For example, an organization may choose to allow most apps ranked as Moderate, but exclude Moderate apps that require access to a contacts list or exhibit other undesirable behaviors. With this level of granularity, the Webroot App Reputation Service is capable of creating a mobile security policy that is tailored to the needs of each individual organization.
5.0 CONCLUSIONS AND RECOMMENDATIONS

With the onslaught of app-borne cybercrime, app reputation services are the only way to effectively protect mobile devices. Mobile device security solutions are necessary at the device, operating system, and application layers, but these approaches need to be augmented with a powerful app reputation service that can effectively combat the growing threat of mobile malware.

When selecting a mobile app reputation service provider, it is important to weigh the vendor’s overall expertise in the security field as well as their understanding of the specific challenges posed by the mobile world. In particular, it is essential to select a mobile app reputation service that:

a. Is constantly kept up-to-date using a comprehensive intelligence network.
b. Is simple to work with and integrate.
c. Provides deep granularity of information and the flexibility to address it.
d. Is easily adapted to meet different security policy needs.
e. Exposes a wealth of information to set policies and analyze trends.

The Webroot App Reputation Service provides MDM vendors, mobile app developers, mobile carriers, and application distributors the ability to deliver and manage mobile applications safely and securely. Backed by the Webroot Intelligence Network, the Webroot App Reputation Service meets all the key characteristics described above and harnesses data from millions of sources, making it one of the most powerful application reputation services on the market. As the number of mobile applications available increases exponentially, Webroot offers assurance that partners and customers are protected from mobile threats.