Webroot Security Intelligence for Mobile Suite

Cloud-based security solutions for mobile management providers
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTRODUCTION</td>
<td>3</td>
</tr>
<tr>
<td>WEBROOT INTELLIGENCE NETWORK</td>
<td>4</td>
</tr>
<tr>
<td>MOBILE SECURITY INTELLIGENCE SUITE</td>
<td>5</td>
</tr>
<tr>
<td>Mobile Android SDK</td>
<td>5</td>
</tr>
<tr>
<td>Webroot Secureweb Browser SDK</td>
<td>7</td>
</tr>
<tr>
<td>App Reputation Service</td>
<td>7</td>
</tr>
<tr>
<td>Summary</td>
<td>9</td>
</tr>
<tr>
<td>About Webroot</td>
<td>10</td>
</tr>
<tr>
<td>Contact Us</td>
<td>10</td>
</tr>
</tbody>
</table>
INTRODUCTION

Mobility currently represents one of the driving factors behind almost all business and IT initiatives. It offers the potential to dramatically enhance business agility, improve employee productivity, and enable major shifts in the way individuals and businesses get work done. In fact, analyst firm IDC concludes that mobility will coalesce with social media, big data and cloud services to form the four pillars of computing’s next dominant platform.

For mobility to fulfill this enormous potential as a business catalyst, organizations must focus on successfully addressing the new security vulnerabilities that mobility creates.

As end-users increasingly rely on smartphones and tablets for their personal and business activities, they store valuable information that is attracting the attention of cybercriminals. This has spawned mobile threats are not only becoming more prolific but also more sophisticated. The behavior of these malicious attacks ranges from stealing confidential data to performing remote control activities such as sending spam or calling premium numbers for cash. Through social engineering tactics, hackers also easily distribute Trojan, spyware and backdoor malware.

In particular, the openness of the Android platform makes it easy for hackers to create and distribute malware quickly, which explains why it has become the biggest target. In the first half of 2012 alone, Webroot Research has seen a 900% growth in Android malware samples, and this rapid growth shows no sign of slowing.

Like desktops, smartphones and tablets are susceptible to digital attacks, but they are also highly vulnerable to physical attacks given their size and portability.

Extending Security Intelligence to Mobile Devices

However, despite all of these significant risks, according to a recent study by Webroot, more than half of businesses said they do not have any solution in place to manage mobile devices and security. IT departments need to secure mobile devices against malicious malware and applications while also protecting corporate (and personal) data in the event devices are lost or stolen. IT administrators also need to centrally manage security for mobile devices as they currently do for their users’ laptops or desktops. These challenges make it critical to implement mobile data management tools that incorporate intelligent security technology.

The Webroot® Mobile Security Intelligence Suite addresses the ongoing, evolving and increasingly dangerous mobile threat landscape. It offers mobile management providers...
security technology that can be embedded within their solutions or delivered as a cloud-based service. The Mobile Security Intelligence Suite (Figure 1) provides the ability to secure devices from malware, malicious web sites and application hijacks. Leveraging threat data gather by the cloud-based Webroot Intelligence Network, technology solutions available for mobile solution providers include Android Security SDK, Application Reputation and a Secure Web Browser. The Webroot Mobile Security Intelligence Suite is designed for integration by Mobile Device Management (MDM) providers, mobile business app developers, device manufacturers, SaaS providers, app stores and security vendors.

WEBROOT INTELLIGENCE NETWORK

The Webroot Intelligence Network (WIN) powers the Webroot Mobile Security Intelligence Suite. WIN collects billions of pieces of information from multiple sources—including data from customers, test laboratories, and intelligence shared between partners and other security vendors—to create the world’s most powerful cloud-based malware detection networks (Figure 2). At 100+ terabytes of threat data and growing, WIN applies Big Data analytics to make highly accurate and timely security decisions—millions of times per day. The Security Intelligence Suite for Mobile utilizes specific crowd-sourced WIN databases such, App Classification, Malware and URL/IP Reputation to power the solution set.

![Figure 2: Webroot Intelligence Network](image)

Webroot Intelligence Network Mobile Security highlights:

- 8.7 Billion URLs, 310 million domains scored and classified
- 100+ TB of PC, Mac and Android malware and virus data—200,000 new PC files per day
- 2 million Android apps, 500K iOS apps analyzed and scored; >200K contain malicious content or present suspicious behavior
- 550 million IP addresses analyzed; >9 million dangerous IPs detected
- Real-time anti-phishing service
MOBILE SECURITY INTELLIGENCE SUITE

The Mobile Security Intelligence Suite comprises an Android SDK, SecureWeb Browser and App Reputation service. Partners can mix and match components, providing the flexibility to choose the security solution that will best complement their mobile management solution.

Mobile Android SDK

Individuals using smartphones and tablets tend to engage in activities that increase the risk of attacks on the business—for example, using social media sites to a greater degree or visiting web sites that may increase vulnerabilities, such as gambling or pornography sites. In addition, mobile devices are more vulnerable to loss or theft, which could put businesses in danger someone outside the organization can access corporate data.

One of the other challenges with smartphones is that users tend to keep them on all the time, even when they are not in use, which further increases their vulnerability to attack. In 2012, Webroot Threat Research saw an exponential increase in Android-based malware threats (Figure 3). Through the end of January 2013, this included over 185K Android malware threats and over 200K Potentially Unwanted Applications (PUA). PUAs include commercial rooting tools, hack tools, aggressive advertising and data leakage apps. IT Admins may consider eliminating the PUAs as they have the potential to impact data loss or incur unwanted mobile usage fees.

For businesses, the security threats that come with increased mobility are not only real, but they are growing rapidly and can cause significant damage. One survey shows that a single breach costs an average of $214 for each compromised record, and the average major data breach event costs $7.2 million. That is damaging enough to put almost any sized company out of business.

Coupled with their exploding growth, inherent weaknesses in smart devices are making organizations much more vulnerable to attack. This means organizations must take steps to ensure that personally owned and company-issued devices are as secure as every other endpoint device connected to the corporate network.

Figure 3: Webroot Threat Research-Android Malware/PUA
The Webroot Android SDK addresses the vulnerabilities of mobile devices by providing mobile management partners the ability to offer security for their customers. The Android SDK is a robust, UI-less mobile security solution providing partners full control over branding and user interface implementation. It features antivirus, antimalware, secure web browsing and URL filtering/content classification. The Android SDK is lightweight and efficient, utilizing very little memory and bandwidth, while maintaining minimal impact on battery life. A fully functional mobile security SDK enables better protection versus a simple blacklist approach that can be provided via cloud based App reputation APIs.

Benefits:

- Industry-leading protection against mobile-based threats
- Does not slow down device or hinder end user productivity
- Secure web browsing blocks malicious URLs and phishing attacks to keep users safe
- Simple and flexible development options for partners

**Android SDK Features**

**Antivirus/Antimalware**

The Android SDK delivers advanced anti-malware detection powered by the Webroot Intelligence Network, the world’s largest and most advanced threat detection system. Deployment options allow for automatic application and file scans for viruses, spyware and Trojans. Antivirus security shields block malware before it has a chance to install.

**Secure Web Browsing URL reputation and IP classification**

Secure Web Browsing uses proprietary Webroot URL content filtering and web reputation databases to prevent users from connecting to malicious sites and phishing attacks. With secure browsing enabled, it will automatically scan web links and URLs to block fraudulent websites other harmful content. Partners also have the ability to filter content based on 85 categories such as gambling, pornography and social networking sites. The feature works with the standard Android browser or can be embedded within a partner's browser.

**SDK Management**

Webroot provides all the tools necessary for partners to complete a simple SDK implementation into their solutions. Webroot partners are responsible for developing all UI components (client and management interface) using the Android SDK. The SDK solution consists of a Java Library, Sample App and documentation. The Compiled Java Library (JAR) is embedded in the partner’s app. The Sample App enables a partner to view how integration of the library could be completed. Documentation details all of the classes and interfaces of the library that enable management control of the settings. APIs allow for full management of all of the SDK security functions. For example, the partner can configure:
• Scan settings
• Definition update frequency
• Real Time Protection settings
• Quarantine
• Threat and URL ignore lists
• URL Category block/ignore lists
• Licensing and installation tracking

Once deployed, security definitions and the URL filtering database are hosted by the Webroot Intelligence Network. Definition updates and URL lookups are performed against the Webroot servers (Figure 4).

**Webroot Secureweb Browser SDK**

In cases where a user goes into Android Incognito mode, protection utilizing URL/content classification is not possible. For this situation, Webroot offers a mobile web browser called SecureWeb. Partners can implement Webroot SecureWeb as the default and only browser used by devices managed by their MDM platform. SecureWeb is a fully functional standalone Android Browser with best-in-class web content classification and reputation. Management of web filtering settings and categories is achieved through an API. With the API, partners can:

• Block a specific URL, category or categories of URLs
• Modify the list of blocked categories
• Ignore a specific URL
• Modify the list of ignored URLs
• Ignore an entire domain
• Develop custom block pages

**App Reputation Service**

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, hackers can easily disguise and distribute malicious code to unwitting victims. In fact, apps have become the primary vehicle to distribute mobile malware, and the exponential growth of apps is compounding the problem. As of September 2012, for example, mobile users had downloaded 25 billion apps from the Google Play Store.

While mobile malware still represents only a fraction of the millions of threats targeting PCs, the number of new mobile threats has shown a more aggressive growth trajectory. Nonetheless, individuals and businesses remain largely unaware of the risks of mobile applications. Most mobile malware is delivered via mobile apps cleverly disguised as “good” and distributed through mobile app markets. Unsuspecting individuals install these applications on their mobile devices without doing any research on the application or its developers, opening the door to an attack with precious data as the target. Moreover, with BYOD becoming a reality, this presents a security threat to individuals and businesses alike.
The large volumes of existing apps, a constant stream of new apps, and a growing number of third-party app distribution markets combine to present a significant security challenge. How do you determine which apps are malicious and which apps are safe? Vendors that provide mobile management and security solutions need to ensure their customers are protected from malicious applications, have the ability to filter out unwanted or non-compliant apps and allow access to reputable applications.

Due to increasing threat presented by mobile applications, Webroot has developed the Webroot App Reputation Service. Utilizing data collected and analyzed by the Webroot Intelligence Network, the App Reputation Service gives Webroot partners and customers the ability to manage the delivery of mobile applications that are safe and compliant.

**How Webroot App Reputation Service Works**

Figure 5 presents a process flow showing how the App Reputation Service collects, analyzes and distributes app data to partners and customers.

1. **Collection.** The App Reputation Service collects millions of applications from app markets, third-party sites, app sharing services, strategic partners, and SecureAnywhere Business—Mobile Protection users.

2. **Analysis.** After the applications are fed into the App Reputation Analytics Engine, an automated, multi-staged analysis process collects detailed data on each application.

3. **Classification and Scoring.** Each app is categorized and assigned a score based on algorithms using detailed analysis data. Compared to simply looking at the permissions that the apps request, 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.

4. **Partner API.** The Classification and Scoring results allow Webroot partners to analyze apps or analyze app data via a web service API.

![Figure 5: App Reputation Service](image-url)
5. Feedback Loop. Information collected by Webroot partners is then gathered and looped back into the App Reputation analytics engine.

6. 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 free from malicious or unwanted mobile apps.

**App Reputation Service API**

Webroot has streamlined application reputation analysis to provide a concise classification and other information on mobile apps in the database. The information collected is exposed via a RESTful web service API and can be used by MDM or other applications that enable mobile app usage policies. Webroot provides several application lookup mechanisms, including package name and md5. A simple banding classification, ranging from Malicious to Trustworthy, provides an easy-to-implement solution for Webroot partners. This is the main advantage of the App Reputation Solution—either allowing or blocking the mobile apps based on the policy designed to safeguard the interest of business and its users.

Developers using the API have flexibility to set permissions beyond the banding classification and use other data points exposed via the API to determine application policy compliance. For example, an app may be classified as moderate, yet it might have other undesirable characteristics such as GPS location or access to user’s phone contact list.

The Webroot App Reputation service allows MDM vendors, mobile carriers, and application distributors to deliver mobile applications safely to their customers. Built on the Webroot Intelligent Network, it harnesses data and inputs from millions of sources, making it one of the most powerful application reputation services on the market.

The App Reputation Service is simple and easy to integrate. It provides flexibility for MDM providers, mobile carriers and app market providers to decide how to use the mobile app information and adapt it for specific management requirements.

With millions of mobile applications available and new apps introduced every day, Webroot partners will have the assurance that their customers are protected from the potential threats hidden in mobile applications and are using only safe apps.

**SUMMARY**

A dramatic shift to a more mobile workforce and business environment is taking place right before our eyes. We are seeing the rise of mobile applications and the use of devices for all types of interactions. In addition, employees are using those same devices for both personal and business purposes—sometimes with the support and approval of the business, but more often without proper safeguards in place. Businesses must face the reality that all of this increased mobility makes their businesses far more vulnerable to security threats. Using Mobile Device Management solutions with best-in-class mobile security is critical to keeping company data and users safe. The Webroot Mobile Security Intelligence, offers mobile management vendors a robust set of mobile security solutions all powered by world’s largest threat intelligence network. Leveraging the Mobile Security Suite, mobile vendors are assured their customers are safe and protected from mobile threats.
ABOUT WEBROOT

Webroot is committed to taking the misery out of Internet security for businesses and consumers. Founded in 1997, privately held Webroot is headquartered in Colorado and employs approximately 350 people globally in operations across North America, Europe and the Asia Pacific region.