WEBROOT
BrightCloud® *Threat Intelligence*
FOR TECHNOLOGY PARTNERS

BrightCloud® Mobile Security SDK

for Android™ and iOS®

OVERVIEW

- From January 2012 through January 2016, the percentage of apps that were malicious jumped from 2% to 17%
- Sites hosting mobile malware, malicious apps, and lost/stolen devices threaten corporate data
- The BrightCloud® Mobile Security SDK offers enhanced mobile security, including antivirus, antimalware, device and application interrogation, secure web browsing, and overall device risk score

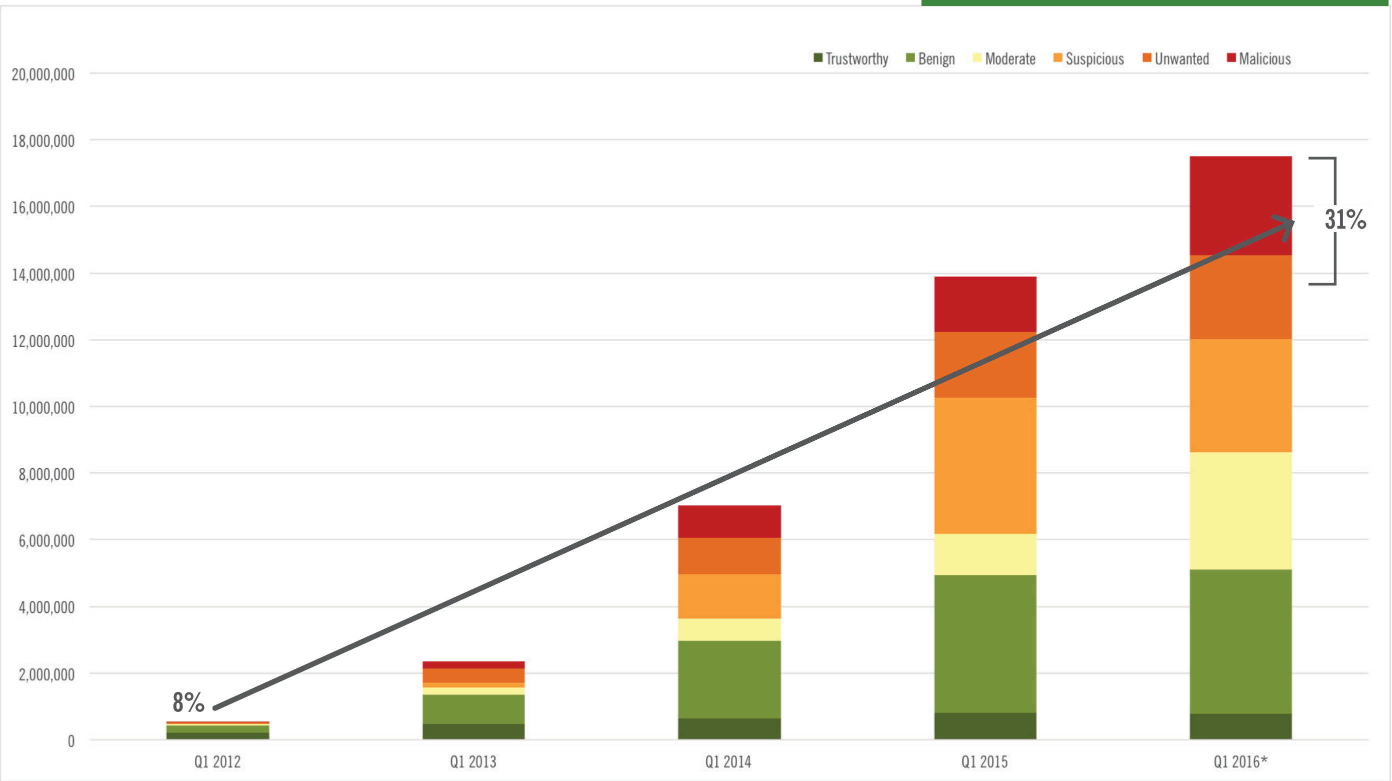
In addition to the massive growth in malicious Android apps between January 2012 and January 2016, the Webroot Threat Research team documented a substantial increase in potentially unwanted Android apps (PUAs). PUAs include commercial rooting tools, hacking tools, aggressive advertising and data leakage apps (Figure 1). Security administrators may consider eliminating PUAs, as they have the potential to impact data loss or incur unwanted mobile usage fees.

Mobile devices are also vulnerable to physical loss or theft, which means a person outside the organization might gain access to corporate data.

In addition, individuals using smartphones and tablets tend to engage in activities that increase the risk of attacks on the business, e.g., using unsecured public Wi-Fi, accessing social media sites to a greater degree or visiting websites that may increase vulnerabilities, such as gambling or pornography sites.

The BrightCloud Mobile Security SDK addresses mobile device vulnerabilities by enabling mobile management partners to offer enhanced security for their customers. It features antivirus, antimalware, device and application interrogation, and secure web browsing, along with an overall device score for administrators to assess the risk levels of devices on their network. The SDK is lightweight and efficient, utilizing very little memory, bandwidth, or battery life. A fully functional mobile security SDK offers significantly better protection than a simple, static blacklist approach.

Figure 1 » Percentage of Android Apps by Reputation



Mobile Security SDK Benefits

- Industry-leading mobile threat protection
- Does not slow device or hinder user productivity
- Secure web browsing blocks malicious URLs and phishing attacks
- Simple, flexible development options for partners

PARTNER BENEFITS

- **Differentiate yourself from your competition**
  Offer your customers industry-leading protection against mobile threats
- **Leverage Webroot® Threat Intelligence**
  Harness collective threat intelligence from millions of sources via the world's most powerful cloud security network
- **Easy integration gives you full control**
  Simple, UI-less integration puts your brand at the forefront of the user experience
- **No impact on user experience**
  Powerful protection with a tiny footprint and minimal battery drain to satisfy your customers

BRIGHTCLOUD® MOBILE SECURITY SDK IN ACTION

The BrightCloud® Mobile Security SDK features several modules. Mobile management partners can choose from an Active Protection Service, a Scanner Service, an Application Information Module, a Device Information Module, secure web browsing, and Device Risk Score.

Active Protection Service (Monitor Service)

This service keeps track of device events. The service can be left running at all times or enabled while the host application is running and disabled when the host application is done. The host application has full control of the monitoring service, i.e., the service can be enabled for the duration of connection to a remote server and then terminated by the host application.

The Active Protection Service can be also used to notify the host application of any files being downloaded, any applications being installed, and any applications being executed. The host application can log these events, show notifications, and take any other custom actions based on these events.

Scanner Service

This service allows the host application to run system-wide antivirus/antimalware scans of files and apps. Scans can be run silently in the background or the host application can set up scanner listeners to provide feedback to the user. Scan results are stored in a single persistent list, which can be used by the host application to interactively quarantine or remove individual files and applications.

Application Info Module

This module provides detailed information about apps installed and running on the device. The interrogated app's data points are configurable by the host application. Some examples are different package attributes, certificate and manifest information, and various network and process related data points.

Device Info Module

This module provides detailed information about the device and operating system for both Android™ and iOS® devices. The BrightCloud Mobile Security SDK can check if the device is in a rooted state or is running in an emulator. It also gathers various hardware statistics and can uniquely identify the device.

Secure Web Browsing with Web Reputation

The Mobile SDK includes secure web browsing, which uses proprietary BrightCloud web classification and reputation intelligence to prevent users from connecting to malicious sites and phishing attacks. With secure browsing enabled, URLs are automatically scanned for harmful content.

Device Risk Score

Provides a simple, flexible, and powerful risk scoring mechanism to ensure Webroot partner and the end user information is secure. When calculating a device score, the user, the device, and the partner's app are all taken into account. The system covers an endpoint and makes a simple go/no-go decision based on risk criteria, such as whether the device is rooted or jailbroken, contains high risk malware, or uses the latest definitions. The various categories are weighted and scores can be adjusted at the partner's discretion, based on their risk tolerance.

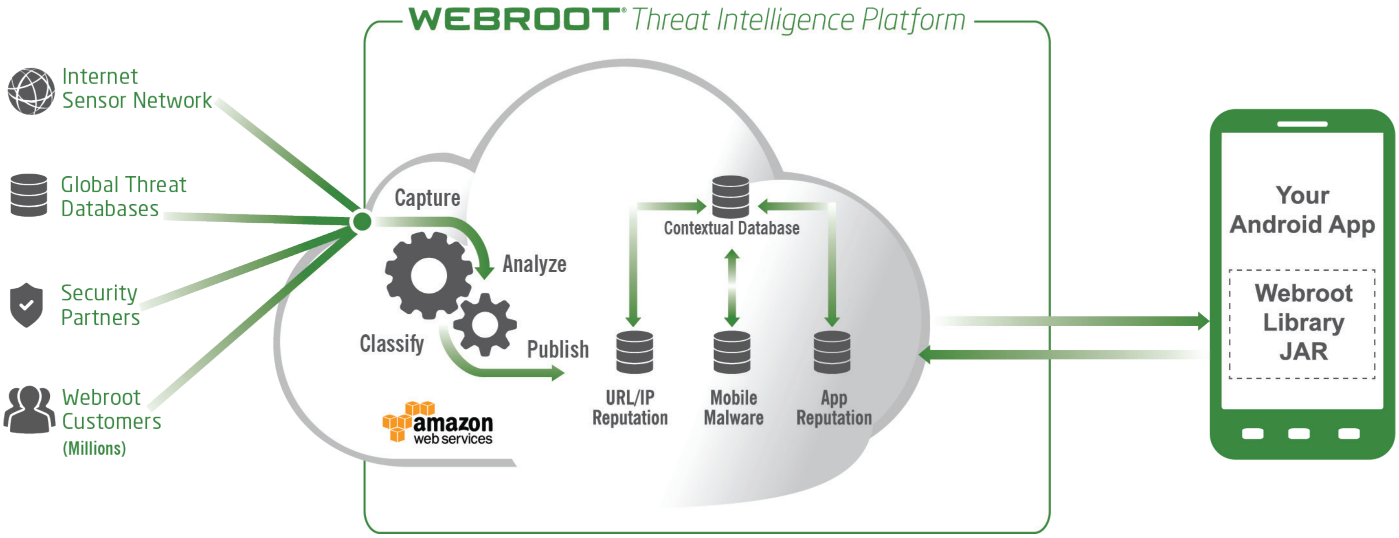


Figure 2 » Security SDK Implementation

Partners have access to all of these services, with the flexibility to leverage any permutation based on their unique needs. This flexibility allows partners to leverage the SDK in various scenarios, such as:

- MDM providers can bolster their customers' mobile security through enhanced protection at a premium rate
- Smartphone manufacturers can differentiate themselves through pre-loaded security for their users, featuring their own brand
- Financial institutions can protect their customers' mobile transactions by ensuring that devices connecting to their network are within acceptable risk levels

Partner Integration Options

Webroot provides all the tools necessary for partners to complete a simple SDK implementation in their solutions. Webroot partners are responsible for developing all UI components (both client and management interface) using the SDK. The BrightCloud® Mobile Security SDK library is modular in design, which allows for a very small memory footprint. Partners enable only the modules needed for their configuration.

The SDK solution consists of a Java Library for Android™ or a header file for iOS®, a sample app and documentation. The Compiled Java Library (JAR) or header file is embedded in the partner's app. The sample app enables a partner to view how integration of the library might be completed. Documentation includes details all of the classes and interfaces in the library that enable management.

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

Once deployed, security definitions and the web filtering database are hosted by the Webroot® Threat Intelligence Platform. Definition updates and web lookups are queried against the Webroot BrightCloud servers (Figure 2).

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