SecureBrain

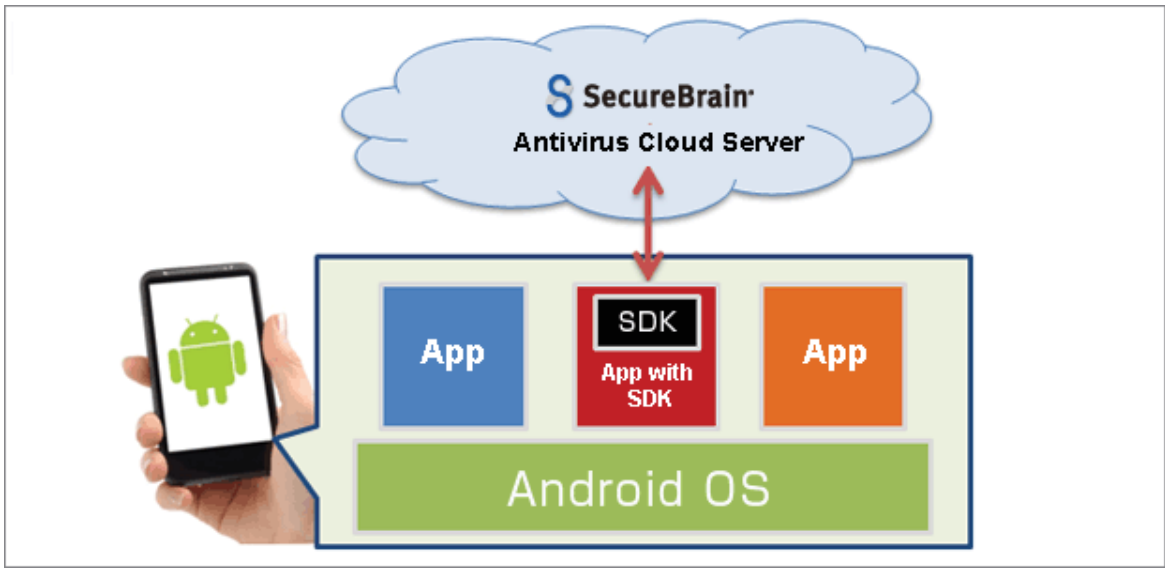
GROWING THREAT OF ANDROID MALWARES

The number of Android malware is growing. As of July 2012, we have identified more than 15,000 unique malware that are composed of 150 malware families including their variants and polymorphic mutations. Such malware is even found on trusted sites like Google Play Store. The market share for Android platform is growing, and Android devices are now being used for security-sensitive apps such as apps for online banking and apps that require connection to corporate internal networks. Thus, there is a more urgent need for antimalware functionality to help ensure that the device is free from malware when using such applicatiaons.

Because of this need, 3rd party developers who build applications need to ensure that the device is malware-free before executing the core functionality of their applications. However, it is not practical or cost effective for most parties to develop and maintain such antimalware functionality, since this would normally require an expert security research team to collect, analyze and develop detection algorithms for thousands of new malware that are discovered regularly.

OUR ADVANCED CLOUD ANTIVIRUS SOLUTION

Cloud Antivirus SDK is a commercial-grade toolkit for Android platform that allows professional developers to easily add antimalware functionality into their applications. It features the patent pending “in-cloud” scanning that offloads CPU and network intensive computations to the cloud to help reduce battery and network usage on the device. All the complex core antimalware functionality is provided and maintained by SecureBrain, thus allowing you to add antimalware functionality easily, more cost effectively, and help reduce your time to market. This white paper provides a technical overview of SecureBrain Cloud Antivirus SDK, the only “in-cloud” antivirus scanning engine for the Android platform.



ANDROID MALWARE LANDSCAPE

In June 2012, Google mentioned that there are a total of 400 million devices, and 1 million Android activations occur each day. There are more than 600,000 apps available for Android, and the estimated number of apps that have been downloaded from Google Play so far is 20 billion.

The first Android malware named AndroidOS.FakePlayer was discovered in October 2010. It was a Trojan horse disguised as a media player app. Upon execution of this Trojan horse, it would discreetly send an SMS message to a premium SMS service without the user's knowledge.

Since the discovery of the first Android malware, new malware threats have grown in number and have become more sophisticated. Some types of malware are able to break into the Android security architecture by exploiting system vulnerabilities. As a result, these malware are able to access sensitive content. There are also malware that target online banking activities by intercepting and stealing online banking SMS transaction codes. These types of malware just mentioned have been found on trusted app markets including Google Play. For example, in April 2012, 31 variants of a malware called AndroidOS. Dougalek were discovered on Google Play targeting Japanese Android users. This malware was estimated to have at least 300,000 downloads. The malware author also leveraged affiliate programs to market the trojanized app to lure more users into downloading it.

According to SecureBrain research, the number of new malware discovered began to increase rapidly in Aug 2011. By July 2012, SecureBrain has confirmed over 15,000 unique Android malware including at least 150 malware families. Each family may be composed of multiple variants and polymorphic samples.

With such an alarming growth rate of malware, it is critical to inspect the device for malware before connecting it to a corporate network or running security-sensitive apps on it such as an online banking app.

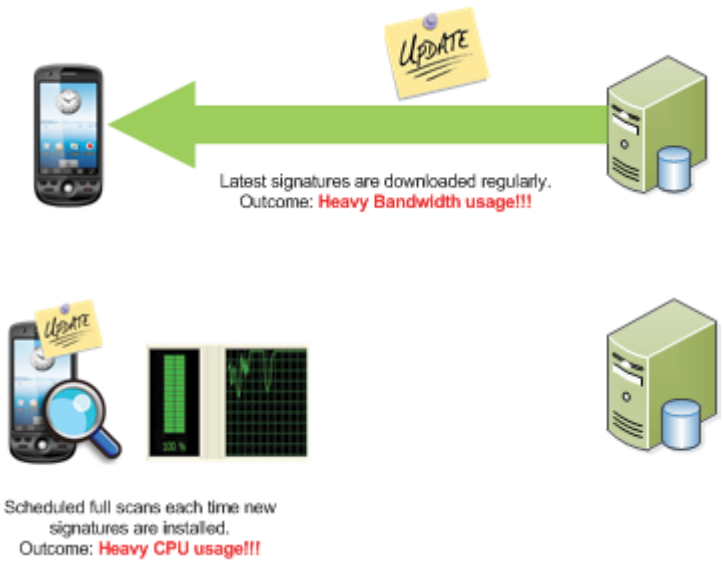
SecureBrain is a security company based in Tokyo that specializes in developing technology to fight Android malware. To keep up with the latest knowledge on malware, SecureBrain networks with leading international security companies as well as domestic research agencies in collecting, analyzing and researching new Android malware.

CLOUD ANTIVIRUS ARCHITECTURE ADVANTAGE

Cloud Antivirus SDK architecture has been specifically designed for mobile platforms to minimize battery drainage and network traffic. To accomplish this, we have moved the CPU and network intensive core functionality to the cloud. To better understand this, we will first describe traditional antivirus architecture and traditional cloud antivirus architecture. Afterwards, we will compare them against our technology so that you can visualize the advantages of using our SDK.

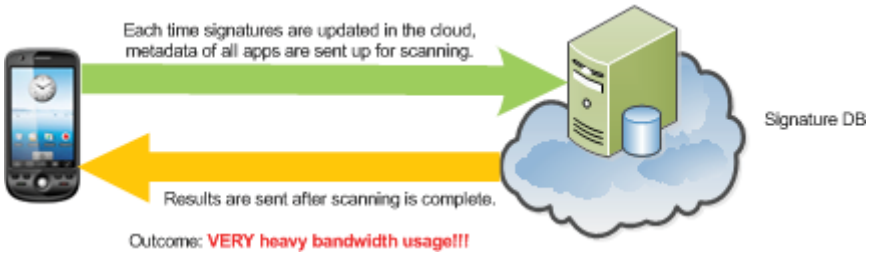
Traditional Antivirus Architecture

Detection signatures are downloaded to the device regularly. Antivirus will scan installed apps and refer to detection signatures to identify new threats. As the number of signature deployment and data size grow, network traffic would also grow. After signatures are deployed to the device, all applications need to be scanned again, thus causing high CPU usage. To be protected from the latest threats, users must constantly download new signature updates. This type of practice is difficult to enforce.



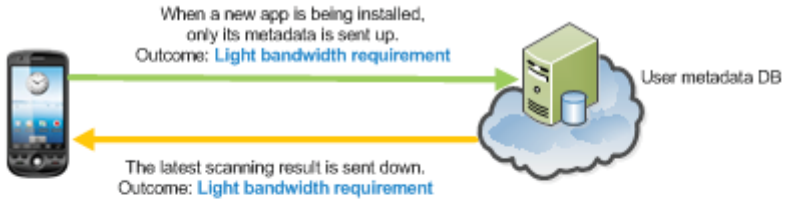
Traditional Cloud Antivirus Architecture

In this architecture, detection signatures live in the cloud. Each time the antivirus scans, it will extract unique metadata of installed apps and send them up to the cloud for determination. By hosting the detection signatures in the cloud, it can ensure that every scan operation uses the latest signatures. Since the signatures in the cloud are periodically updated, the antivirus client will need to perform periodic scans. With the alarming number of new malware found, signatures are constantly updated, thus the device is required to perform periodic scans frequently, which can cause a faster battery drain on the mobile device.



SecureBrain "In-Cloud" Antivirus Architecture

Similar to traditional cloud antivirus architecture, the detection signatures live in the cloud. However, what makes our architecture unique is how we manage the metadata of all the installed applications on users' devices. Rather than sending the metadata to the cloud each time a file is scanned, we send the metadata when applications are "installed" on the device, and it is sent only once during the installed app's lifetime. The metadata is then managed by our cloud. Each time detection signatures in the cloud are updated, the metadata stored in the cloud are automatically re-scanned. This is why it is called "in-cloud". There is no need for the client to scan on the device each time signatures are updated. When an app is determined to be malware, our cloud can provide that information to the device. This patent pending architecture was designed to limit network traffic and CPU usage, which is a critical concept on mobile platform applications. This architecture also allows us to scan applications that may have been already uninstalled from the device.



Device can stay idle while the cloud is updating its signatures and re-scanning users' metadata.

New signatures have been posted. Cloud server will re-scan the entire user metadata database. All the work is performed on the cloud.

FEATURES & MAIN BENEFITS OF OUR CLOUD ANTIVIRUS SDK

- **"in-cloud" architecture offloads complex functionality to cloud**
  - o Complex scanning functionality are all implemented at the cloud and maintained by SecureBrain.
  - o No detection signature file deployment to the device is needed.
  - o No scheduled scan is needed on the device since all applications are automatically scanned in the cloud each time signatures are updated.
  - o Offers recall detection of uninstalled apps.
- **Mobile friendly**
  - o Low battery consumption
  - o Minimum network traffic used for scanning
- **Comprehensive Sample and documentation**
  - o SDK and API documentation in English and Japanese
  - o Full source included for sample antivirus app
- **Easy to use API**
  - o Collect and upload app information
    - Extract metadata from installed app.
    - Send metadata up to the cloud.
    - All metadata will be scanned in the cloud.
  - o Query Cloud
    - Get malware determination from cloud.

ADVANTAGES OF OUR IN-CLOUD ANTIVIRUS SDK

	Traditional Antivirus	Traditional Cloud Antivirus	SecureBrain In-Cloud Antivirus SDK
Android Malware Scanning	✓	✓	✓
Heuristics Detects new threats with generic signatures	✗	✓	✓
Real-time Signatures Always scan with the latest signatures	✗	✗	✓
Recall Detection of previously installed apps	✗	✗	✓
Power Saving Feature #1: After signatures are updated in the cloud, scheduled scan that can cause excessive use of processing power is no longer required.	✗	✗	✓
Power Saving Feature #2: When new signatures are posted, a full re-scan on the device is no longer required. Newly discovered threats on the device are still caught automatically.	✗	✗	✓
Power Saving Feature #3: Downloading signatures that cause excessive use of networks bandwidth is no longer required.	✗	✗	✓

SAMPLE APP INTEGRATION EXAMPLE

Cloud Antivirus SDK includes a sample antivirus application will complete source code to help you get started quickly. Developers using this SDK are welcomed to recycle any parts of the source code. To better explain the concepts on how to use the SDK properly, we will discuss its design in four major parts. Each part is clearly demonstrated on the sample application.

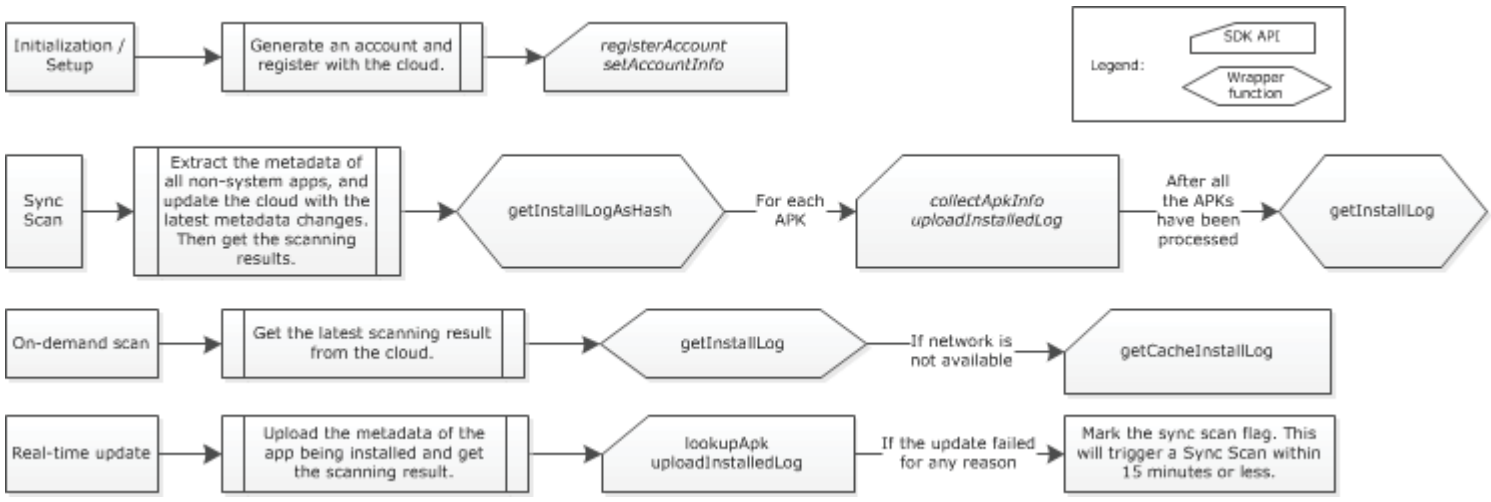
Initialization / Setup: Your app has been installed on the user's device for the very first time. Your app will use the SDK to automatically create a new account and store the account information locally. Each time an SDK instance is created in your app, the account info needs to be set into it to allow the SDK instance to communicate with the cloud.

Sync Scan: The main concept for this step is to update the cloud with the latest set of metadata of non-system apps that have been installed or uninstalled on the device. It is recommended that this step is performed in the background. The first time that this is performed on the sample app is immediately after cloud registration succeeded. It needs to extract metadata for all non-system apps that have been installed or uninstalled on the device. This can be easily accomplished by using the Android built-in Package Manager. Metadata retrieved for every app would then be uploaded to the cloud. After the entire process is complete, your app can check the cloud scanning results to ensure that the device is free of malware before proceeding. During the successive calls to Sync Scan, the device will only update the cloud the new changes on the set of metadata. This is to avoid unnecessary network usage that can drain power resources.

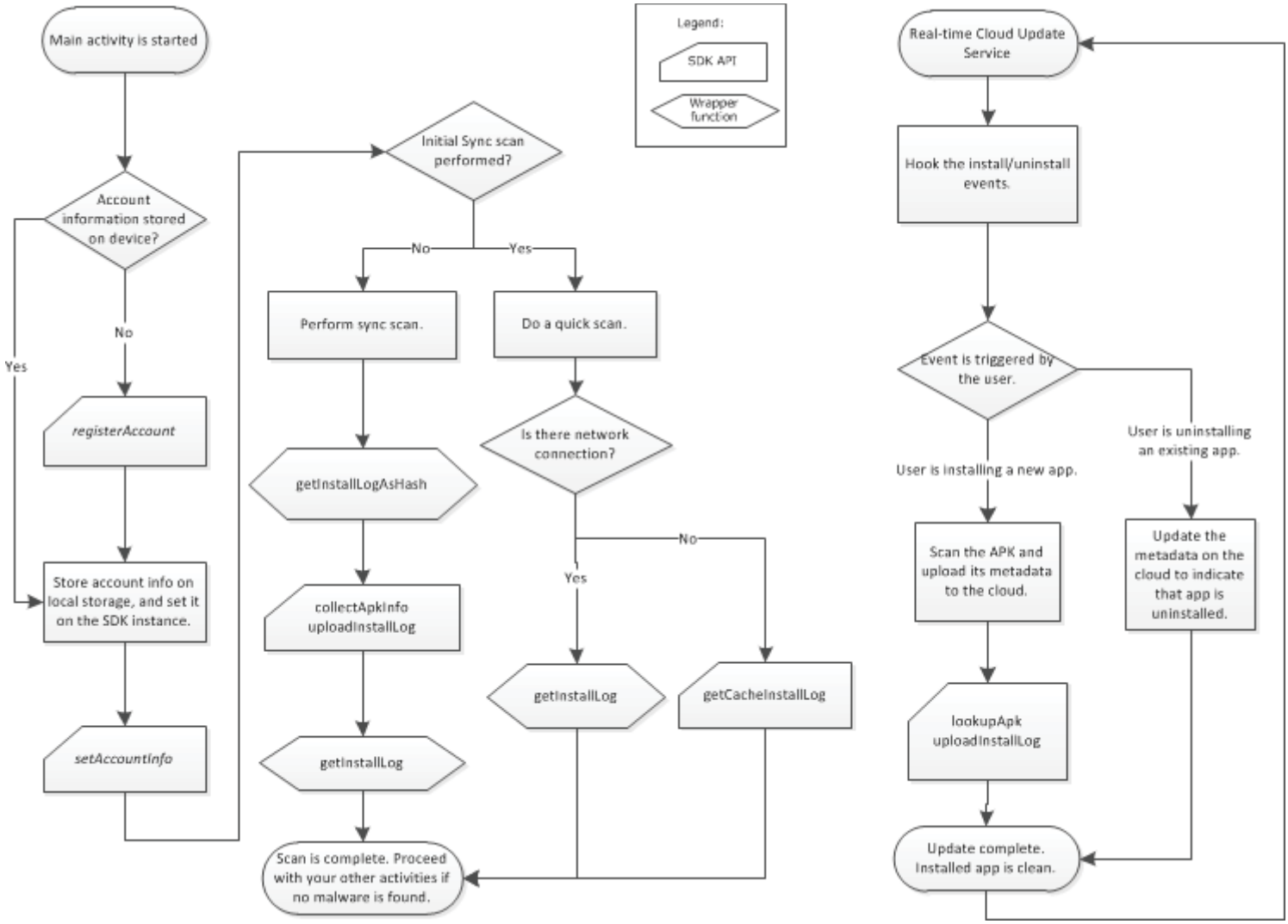
On-demand Scan: This process is extremely fast since all the analysis and scanning have already been performed on the cloud with the metadata that was uploaded in the previous step. Thus, when your app invokes an on-demand scan request, it would simply retrieve the logs from the cloud.

Real-time Updates: A user may install new apps or uninstall existing apps on the device. Your app should also include a service component that will have a handler for these events. When such events occur, you can use the SDK to automatically extract metadata of the app being installed or uninstalled, and upload this metadata automatically to the cloud. This ensures that the cloud always has the most updated logs so that it can provide accurate scanning results to your device. If this activity failed due to network problems, the recommended course of action is to schedule a Sync Scan within a short period of time.

Flow Chart On The Design Of The Sample Application



Flow Chart On How You Would Use the SDK On Your Own App



SecureBrain

Basic Features In Sample Applications

The chart below outlines the basic feature included in the sample app. Our sample application already includes the complete source code and project files for a fully functional antivirus sample application. Developers are encouraged to leverage any parts of the source code or project files in any way that would help them reduce the development time required.

Application	Cloud Antivirus SDK API
Initialization / Setup	registerAccount setupAccountInfo
Sync Scan	getInstallLogAsHash collectApkInfo uploadInstallLog getInstallLog
On-demand Scan	getInstallLog getCacheInstallLog
Real-time updates	lookupApk uploadInstalledLog

Wrapper Functions

Here is a brief explanation of the wrapper functions that were created to simplify the usage of the SDK.

- **getInstallLog (wrapper function)**
  - o Obtains the latest metadata including scanning results from the cloud. Automatically notifies the user if malware is detected.
  - o Uses the following SDK APIs:
    - getCacheInstallLog
    - getInstallLog
- **getInstallLogAsHash (wrapper function)**
  - o Obtains the latest metadata including scanning results from the cloud in a <HashMap> object. Automatically notifies the user if malware is detected. This is used for optimizing the comprehensive uploading of metadata during Sync Scan.
  - o Uses the following SDK APIs:
    - getCacheInstallLog
    - getInstallLogAsHash

Technical Details Of Each Process

We will now describe the APIs and wrapper functions involved in each process.

Initialization / Setup:

- registerAccount
    - o Generates an account automatically. Your app should store the account information locally for future use.
- setupAccountInfo
    - o Retrieve the account information that was stored and use this API to apply it to the SDK instance. This allows your SDK to communicate with the cloud.

Sync Scan:

- getInstallLogAsHash (wrapper function)
- For each APK information in the Package Manager
    - o collectApkInfo
    - o uploadInstallLog
- getInstallLog (wrapper function)

On-demand Scan:

- getInstallLog (wrapper function) – if network is available
- getCacheInstallLog – if network is not available

Real-time Updates:

- For each APK that is installed
    - o lookupApk
    - o uploadInstalledLog

Specifications

Cloud Antivirus SDK support the following platforms
Client Platforms: Android OS 2.1 or above (ARM processor)

Access Methods

User Permission	Description
android.permission.WAKE_LOCK	For control in the power-saving mode
android.permission.RECEIVE_BOOT_COMPLETED	Terminal boot completed event hook
android.permission.VIBRATE	Vibrate
android.permission.INTERNET	Network connection
android.permission.WRITE_EXTERNAL_STORAGE	Write access to the SD card
android.permission.ACCESS_NETWORK_STATE	Access to the network connection state

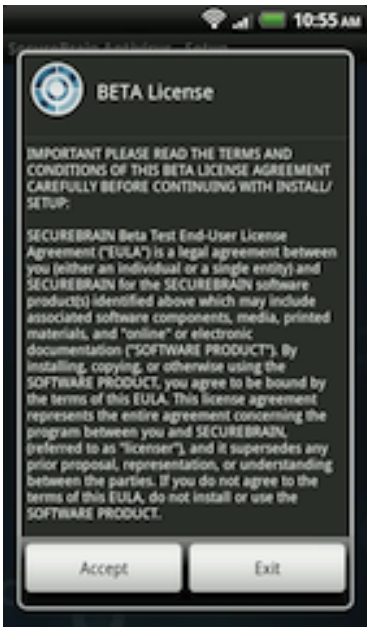
SECUREBRAIN ANTIVIRUS BETA FROM GOOGLE PLAY

Our company has developed an Android antivirus application using this SDK, and has made its beta version available for FREE at Google Play to demonstrate the power of our SDK. You may install the SecureBrain Antivirus Beta from the following location:

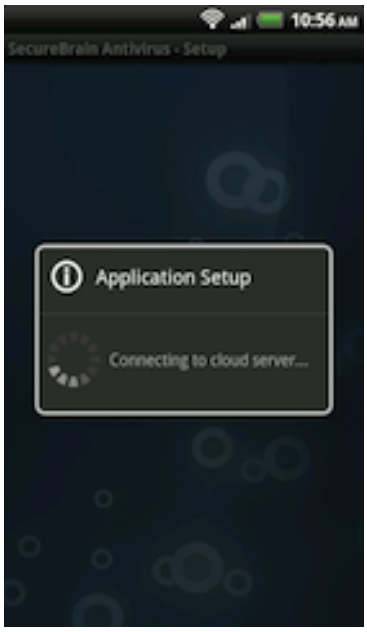
https://play.google.com/store/apps/details?id=jp.co.securebrain.Antivirus&hl=en

SCREENSHOTS OF SECUREBRAIN ANTIVIRUS BETA USING THE SDK

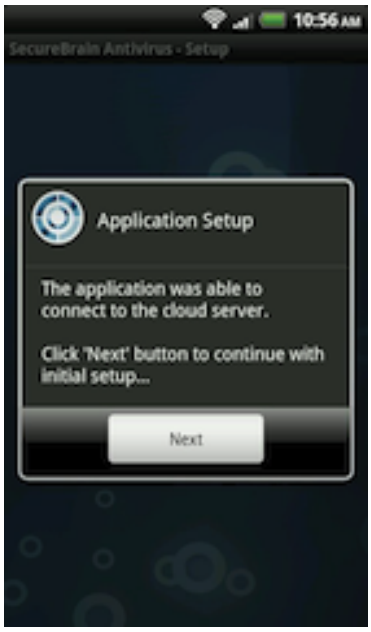
Initialization / Setup



EULA Agreement



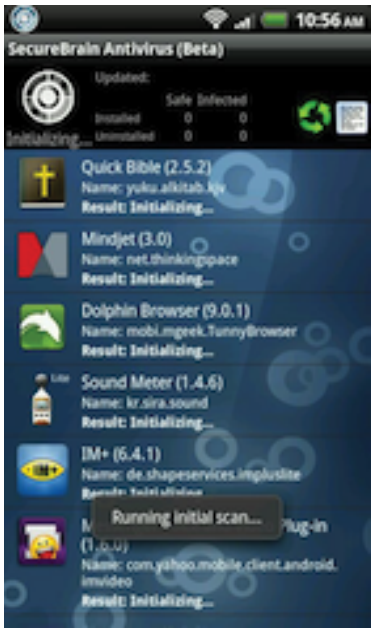
Registration with Cloud Server



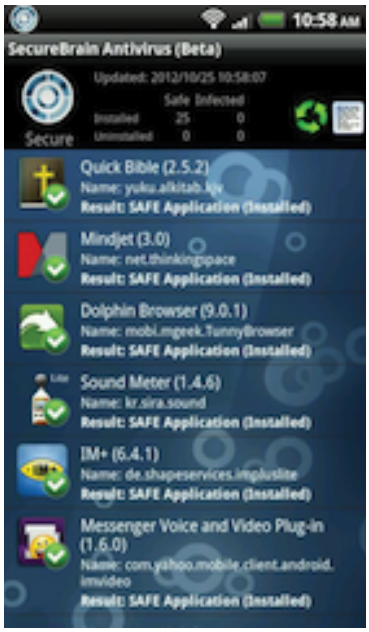
Registration Success

Sync Scan

Initial Scan to Begin



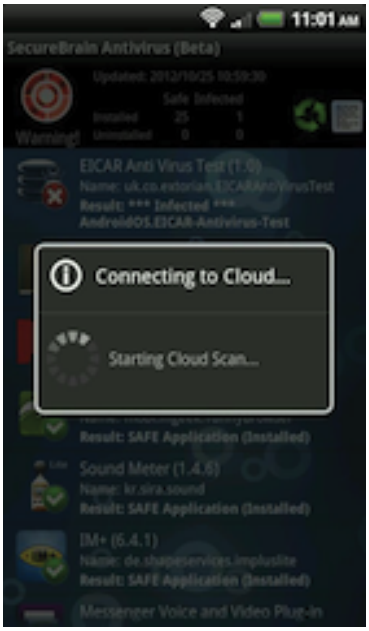
Initial Scan in Progress



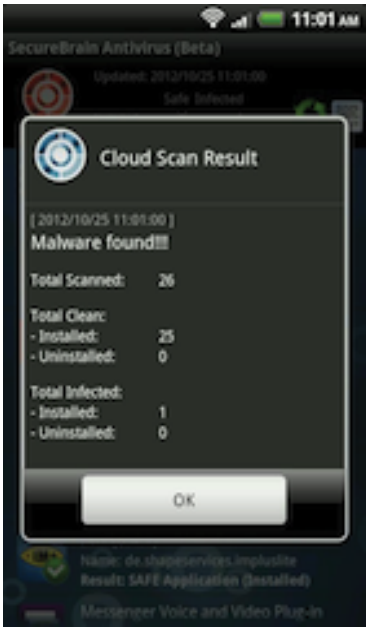
Initial Scan Finished

SCREENSHOTS OF SECUREBRAIN ANTIVIRUS BETA USING THE SDK

On-demand Scan



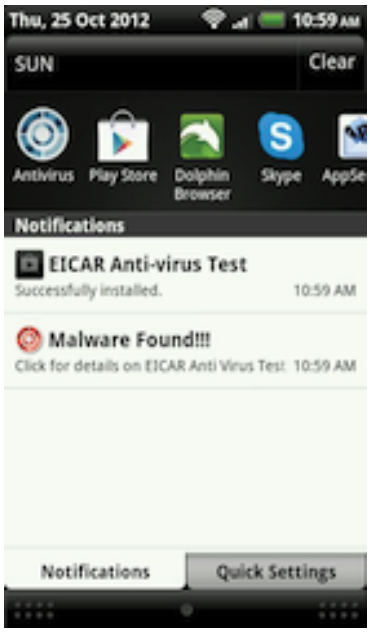
Retrieving Latest Cloud Scan Results



Displaying Cloud Scan Results

Real-time Updates

Test Virus Installed &
Alert Notification Displays on Top



Alert Notification

Option to Uninstall Detected App

SecureBrain®

Cloud Antivirus SDK

For Android Smartphones & Tablets

ABOUT US

Based in Tokyo, Japan, SecureBrain is a leader in providing high quality security software and services. Our software and services help protect our customers against Japanese specific cybercrime as well as global internet security threats such as online fraud, drive-by downloads and malware attacks. SecureBrain is also a government contractor specializing in cyber security and has consistently been awarded numerous contracts every year by the Japanese government.

CONTACT US

SecureBrain Corporation
Web: http://www.securebrain.co.jp/eng
Email: info.intl@securebrain.co.jp
Address: Kojimachi RK Building 4F, 2-6-7 Kojimachi, Chiyoda, Tokyo, JAPAN 102-0083