TRUSTLOOK SECURE ai

MOBILE DEFEND

Powering Robust Mobile Security Solutions

TRUSTLOOK

Table of Contents

Introduction

The Growing Threat of Android Malware

The market share for the Android platform is growing, and so too are the number of Android malware. There are currently over 1.5 billion devices running the Android operating system. Along with all those devices come millions of Android malware samples. These staggering numbers creates an urgent need for anti-malware functionality. Many Android devices host security sensitive apps such as payment and banking apps. This only adds to the need to keep these devices protected from threats.

Third-party developers need to protect a device before executing the core functionality of their applications. It requires an expert security research team to create and maintain anti-malware functionality. A team must collect, analyze, and develop detection algorithms for thousands of new malware. Therefore, it is neither practical nor cost effective for the developers do this themselves. In terms of both practicality and cost, the best option is to use a third-party security solution that already has this capability.

TRUSTLOOK SECURE^{ai} MOBILE DEFEND

Trustlook SECURE^{ai} Mobile Defend is a robust, feature-packed, and multi-layered security framework for building mobile security apps, or injecting security protection into existing mobile applications. It is delivered primarily through an SDK. There are seven core components of the SECURE^{ai} Mobile Defend SDK. (See Figure 1) These include virus scanning, anti-pirating, and URL filtering. By leveraging these components, developers are able to provide their customers with the protection needed to keep their smart devices and valuable data secure.

The SECURE^{ai} Mobile Defend SDK provides partners full, but flexible control over branding and user interface implementation. The SDK is lightweight and efficient. It utilizes little memory and bandwidth, while maintaining minimal impact on battery life. The SDK uses an offline database with a small footprint for its signature updates.

Who Uses the SECURE[ai] Mobile Defend SDK?

There are three primary categories of app developers who utilize the SDK:

1. Developers looking to build their own security app

   Security continues to be a major issue on mobile, and many developers want to develop apps addressing these issues. Unfortunately, developing proper security is not easy. It takes vast expertise and resources to identify and fend off malware attacks. Developers can't simply jump from creating a game app to creating a security app. Most developers are not security experts, nor do they need to be. They want to work with a turnkey solution that provides the security component. Doing so allows them to use their expertise to build a differentiated and compelling front end.

2. Developers looking to build security into their non-security app

   There are over 2 million apps in the Google Play store, and most of these apps are not in the Security category. However, all of these apps need to be secure. Or at least ensure those who use them are secure.

   Security is crucial to the experience of all mobile users. Developers understand that incorporating security into their already-existing app is a great way to differentiate their product and offer a better experience for their users.

3. Developers looking to replace their existing mobile security SDK

   Some developers have already created standalone security apps. Others have integrated a security SDK into their existing non-security app. But both of their results vary. What we have discovered is that many of these developers are looking for an alternate solution. They are searching for a mobile security SDK that is comprehensive, powerful, and able to provide greater flexibility when it comes to implementation.

How it Works

One SDK, Multiple Opportunities

The SECURE[ai] Mobile Defend SDK is a small file (60KB). It requires minimal system resources, particularly when compared to a traditional Security/Malware SDK. Yet, Trustlook's SDK offers the highest potential coverage in the industry.

The Trustlook SDK features six different modules that app developers can draw upon to make their products more secure. By integrating these protection features into their native mobile applications, developers can protect their users from the latest mobile attacks.

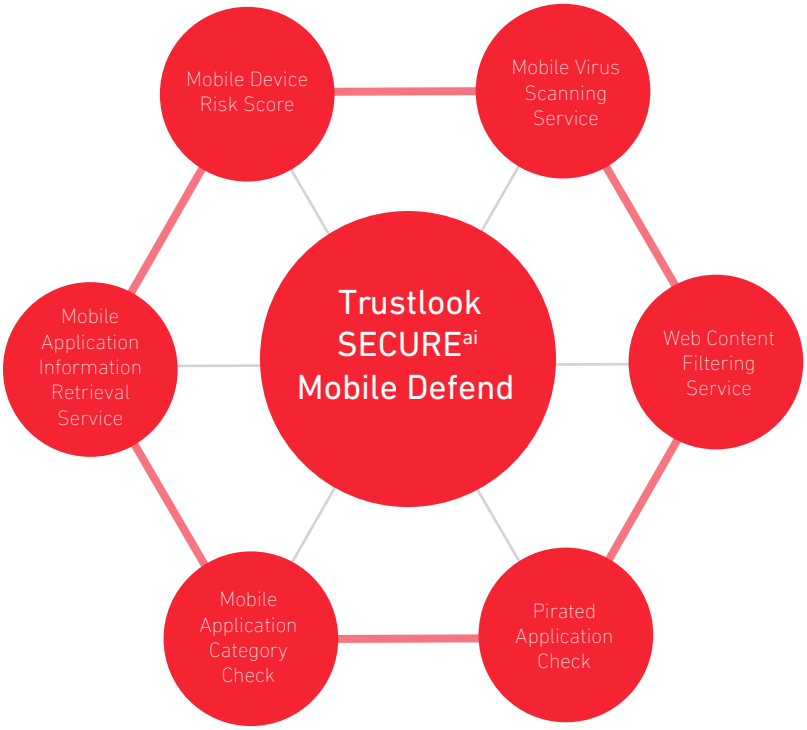


Figure 1: The six modules of the SECURE[ai] Mobile Defend SDK.

Mobile Device Risk Score

Users receive a comprehensive device security score for phones or tablets to indicate whether a device is safe. The score analyzes the device's configuration and vulnerability, and the security data from applications.

Mobile Virus Scanning Service (See Figure 2)

Trustlook provides APIs for scanning system applications and user applications. These APIs provide industry-best detection rates against malware. They are able to handle a high volume of transactions and hundreds of millions of sessions daily. They can detect and analyze different file formats of Android malware, such as APK, DEX, ODEX, and ELF. They can also detect the installation packages and recognize/parse executable files.

Web Content Filtering Service

Trustlook offers an industry leading filtering API for native Android browsers. This API protects against websites related to spyware, pornography, gambling and other potentially malicious content. Trustlook's technology scans all URLs visited by your customers for malicious content. This scan occurs in the split second between the click and visit, guaranteeing customers the ability to securely surf the web.

Trustlook uses a variety of sources to gather and classify malicious URLs. It has its own collection of malicious binaries and the use of industry partners. In total, Trustlook has amassed a large URL database of over 2 billion web pages, adding over 80,000 malicious web URLs daily.

Powered by Maximum Entropy Discrimination (MED) machine learning technology, Trustlook categorizes web links with a high degree of accuracy. Trustlook sorts websites into 78 categories across 9 groups. Developers can filter content at either the Category or the Group level. The web content filtering backend is also highly scalable, and able to handle hundreds of millions of API requests every day.

Pirated Application Check

Pirating and repackaging is a modern-day plague upon the Android app world. Demand for Android applications is growing, but demand for pirated applications grows even faster.

Users are constantly enticed to install apps from non-reputable third-party app stores.

Today's ease of decompiling and hacking Java code makes official license verification libraries susceptible to a hack. Even Google's library has become trivial for hackers to decompile. BORE (break-once-run-everywhere) scripts enable the widespread piracy of applications, and can quickly decimate revenue.

The SECURE[ai] Mobile Defend SDK scans apps on a user's device and verifies the application is from the original developer, not re-packaged by a malicious developer.

Mobile Application Category Check

Bolstered with an extensive Android app inventory and sophisticated data mining processes, Trustlook is able to provide complex insights into individual apps. Trustlook provides REST APIs to most published Android app's detail information.

Mobile Application Information Retrieval Service

Trustlook offers APIs for extracting all types of application information. Developers can retrieve information for both installed system applications and user applications. This information includes permissions, behaviors, and risky API calls.

Figure 2: Trustlook's Mobile Software as a Service (MSaaS) Cloud, the world's largest and most sophisticated threat detection system, is the foundation for the SECURE[ai] Mobile Defend SDK. The above diagram illustrates the SDK's Mobile Virus Scanning process.

Case Study: GO Security

Creating an Entirely New Security App

Sungy Mobile operates the GO series apps, including GO Launcher, GO Keyboard, GO Locker, and GO SMS Pro. In total, the company has acquired over 500 million users across all of its apps. In early 2016, the company wanted to develop a mobile security app. They evaluated several options during the investigative and development phase.

Sungy Mobile realized early on they were an app developer, not a security company. They did not have the resources nor the in-house expertise to create a security app from scratch. The company needed a partner. After months of evaluation, Sungy Mobile chose Trustlook's fast and lightweight mobile security technology. They implemented the SECURE^{ai} Mobile Defend SDK as the foundation of their new security app, aptly named GO Security.

Sungy Mobile's GO Security app provides comprehensive security and privacy protection to users. It offers users the benefits of Trustlook's robust malware detection platform. It also offers security features such as Payment Protection and ID Theft prevention.

Having been around for only a few months, GO Security has become immensely popular. It ranks as one of the top apps in the personalization category in the Google Play store, with millions of downloads and a high user-satisfaction rating.

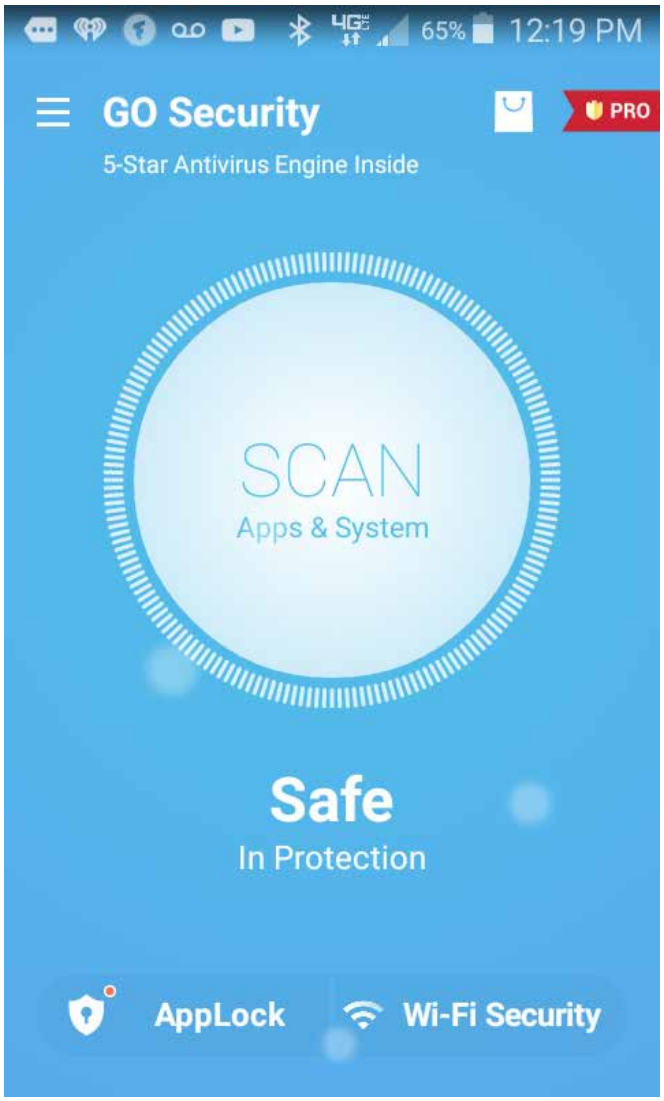
"The partnership with Trustlook is working out amazingly well. We chose to work with Trustlook because of its innovative security platform and broad set of features."

Tao Zhu
Vice President of Technology
Sungy Mobile

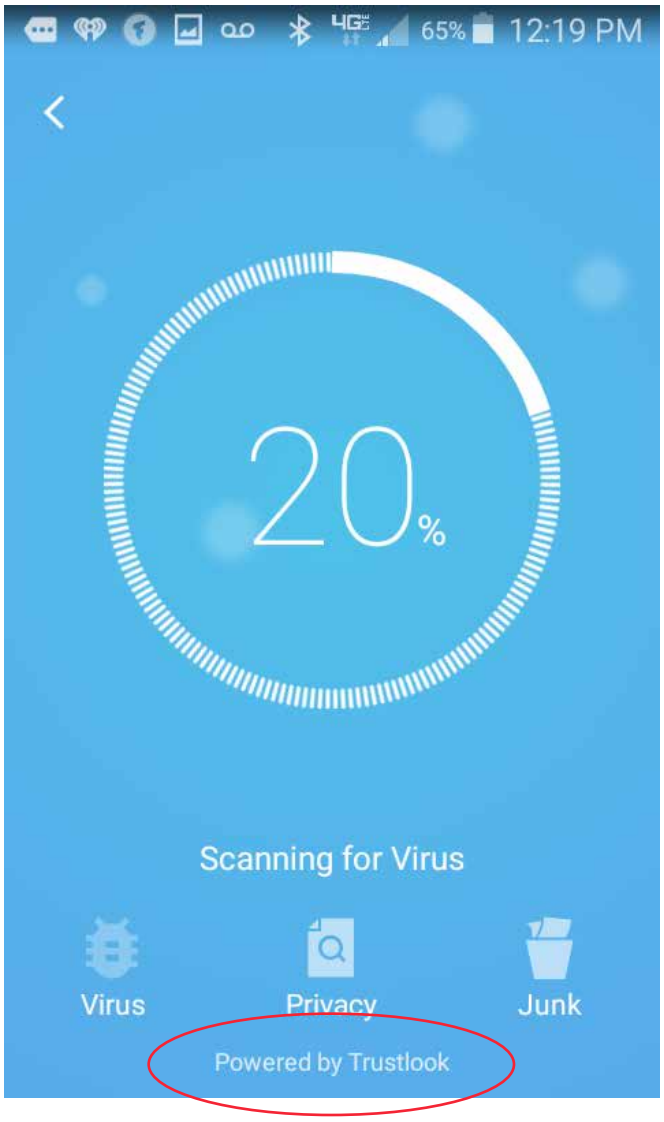
"The GO Security app is a significant development for how Trustlook works with organizations. The Trustlook SECURE^{ai} engine is already embedded within many leading apps, and now with GO Security, Trustlook's technology has been used to create an entirely new app."

Allan Zhang
Founder and CEO
Trustlook

Trustlook affords Sungy Mobile the ability to create its own custom look and feel for GO Security.



The Trustlook SECURE[ai] Mobile Defend SDK powers virus scanning in the GO Security app.



To learn more or schedule a demo of Trustlook SECURE[ai] Mobile Defend, please contact **bd@trustlook.com**.