appthority
TRUST YOUR APPS

MOBILE APP REPUTATION REPORT

Summer 2014

WHITE PAPER

appthority
TRUST YOUR APPS

Introduction

The Appthority® App Reputation Report for summer 2014 provides an overview of the security risks behind the most popular mobile apps. For this report, Appthority App Risk Management Service analyzed the behaviors of Top 400 mobile apps: the top 100 free apps and 100 paid apps for both of the most popular mobile platforms, iOS and Android. The findings were compared against the data collected in the Summer 2013 report to provide broader insight into the evolution of the app economy and provide commentary on current app security trends.

This year Appthority witnessed consistent risky app behaviors across both platforms and compiled the Top 10 Risky App Behaviors that put consumers and businesses at-risk. Appthority determined that the top risky app behaviors most often fall into one of two categories: sensitive data being captured and sensitive data being shared with third parties.

What kinds of data are the most popular apps capturing and where is that data going? This report explains how risky apps access user and corporate data from mobile devices and how that data could be potentially misused. Appthority also examines which third parties are receiving or buying data.

In the ongoing battle to determine which platform is more secure, iOS and Android are now nearly equal when it comes to the risky behavior of the top free apps. However, paid iOS apps surprisingly collect more data and share that information with more third parties than Android paid apps, making iOS slightly more risky than Android when it comes to data sharing. On the whole, free apps remain the most risky category, exhibiting the greatest number of risky behaviors across both platforms.

Risky mobile app behaviors are not only a significant risk to end-users, they also pose significant threats to organizations. With more employees using their own mobile devices and apps for work (BYOD – Bring Your Own

Figure 1a. Top FREE Apps with Risky Behaviors: 100 iOS and 100 Android

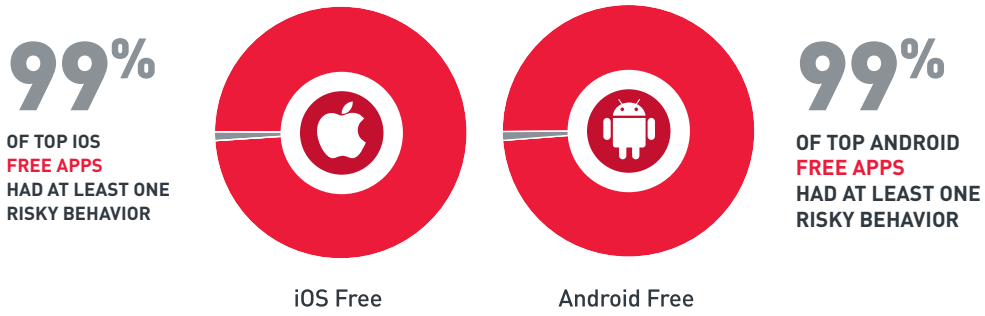
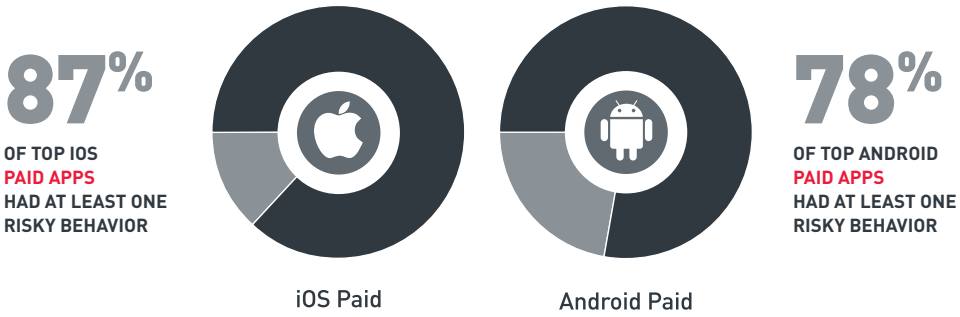


Figure 1b. Top PAID Apps with Risky Behaviors: iOS and Android



Device and BYOA – Bring Your Own Apps), both personal and corporate data intermingle on a single device. As the Top 10 Risky App Behaviors demonstrate, sensitive data is frequently up-for-grabs for third parties to misuse.

Which apps organizations allow employees to use and which ones are deemed too dangerous depends on the employer's tolerance for risk. The first step is understanding the hidden risky behaviors behind the most popular apps. With app titles in the top 100 constantly changing it is important to continuously monitor the app ecosystem for new app titles as well as changing versions. With millions of net new apps created almost every month just from new versions of existing apps, risk analysis of the top apps can quickly become outdated and stale if not continuously monitored.

The Appthority Service is the industry's first fully automated direct-to-enterprise solution for organizations to measure the total risk of public and private apps in their environments within minutes. The SaaS-based service allows IT and security administrators the flexibility to create and manage mobile app policies by company department, by geography or even by device type — whether company or employee owned. This includes approving and enforcing custom, acceptable use polices at scale, and supporting the creation and implementation of multiple group and role-based policies simultaneously.

Additionally, the Appthority Service includes detection for cloud-based file storage violations, a priority for enterprises combatting "Rogue IT." Organizations may sign up directly with Appthority for instant access to the world's largest database of more than two and a half million analyzed apps and obtain new insights into risky app behaviors, privacy issues and mobile malware. Enterprises may also upload new and homegrown apps and obtain app reputation and risky behavior reports in minutes.

Testing Methodology for this Report

The cloud-based Appthority App Risk Management Service performed deep dynamic and behavioral app analysis on the most popular free and paid apps on the iOS and Android platforms. Appthority analyzed each app for particular behaviors within a test environment. Some of these behaviors include location tracking, sharing data with advertising networks or analytic frameworks, accessing and sharing the user's contact list or address book, accessing the user's calendar or in-app purchasing. Appthority also examined apps for these behaviors: identifying the user (or the Unique Device Identifier, UDID) and single sign-on (SSO) support via social networking site integration.

Although malicious software (malware) created to compromise device security or data is portrayed as the principal villain in the mobile application security narrative, malware is not the primary threat to user privacy or enterprise security on mobile devices because it is seldom found on enterprise devices.

Enteprise security teams should not only monitor apps for malware, but also monitor how mobile apps are handling personal info and company data as those apps are often present on employee devices. Appthority's deep analysis into app behaviors actually proves that mobile malware infects only .4% of mobile apps in the enterprise and 0% of apps found in the Top 400.

Report Highlights

Overall, most free apps on both OSs exhibited at least one of the Top 10 Risky Behaviors discussed in this report: risky behaviors were found on 99% of iOS free apps and 99% of Android free apps

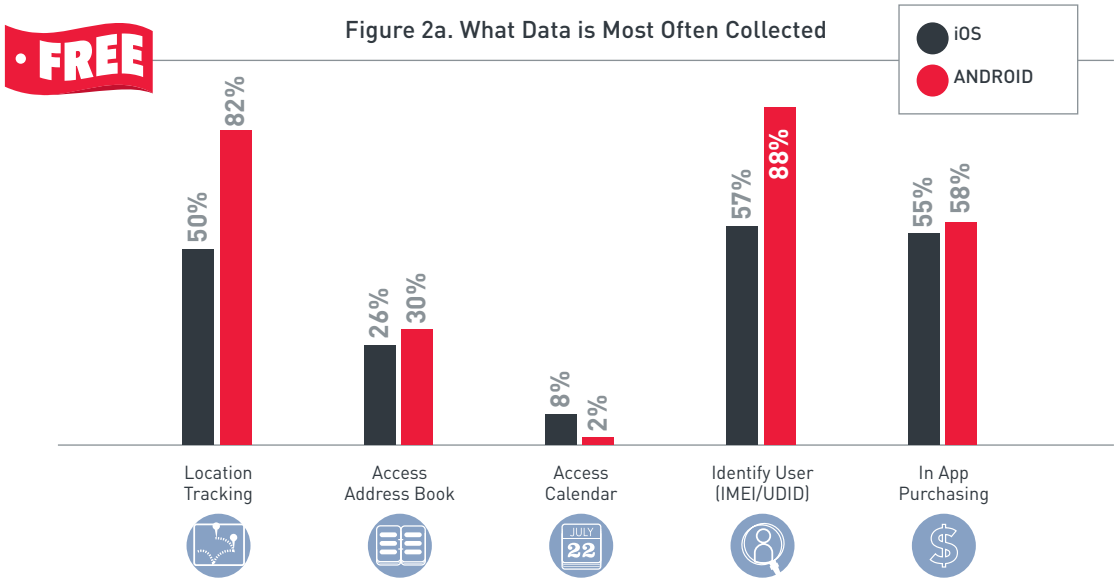
- 78% of the top Android paid apps had at least one of the Top 10 Risky Behaviors
- 87% of the top iOS paid apps had at least one of the Top 10 Risky Behaviors
- 82% of free Android and 50% of free iOS apps allow location tracking
- 88% of the top free Android, 65% of paid Android apps access the user's ID (UDID) compared to 57% of free iOS and 28% of paid iOS apps
- 71% of free Android apps share data with ad networks up from 58% of free Android apps earlier this year
- 58% of the top free Android apps and 55% of the top free iOS apps allow for in-app purchases
- 31% of the top free Android apps connect to cloud file storage, compared to 16% of free iOS apps

appthority
TRUST YOUR APPS

Top 10 Risky Behaviors

Are free apps really "free"? Appthority found that the popularity of free apps continues to come at the price of privacy and security. App developers are increasingly funding their free apps by sharing user data with third parties, such as advertising networks and analytics companies, with some developers being paid more for collecting and sharing more data. With high risks of exposing security, privacy and financial info, Appthority determined where the data collected by apps is going, which third parties are buying the data and the potential risks of the transaction. Additionally, a growing number of both free and paid apps allow for in-app purchases.

Figure 2. Top 10 Risky Behaviors: Data Collection and Where the Data Goes



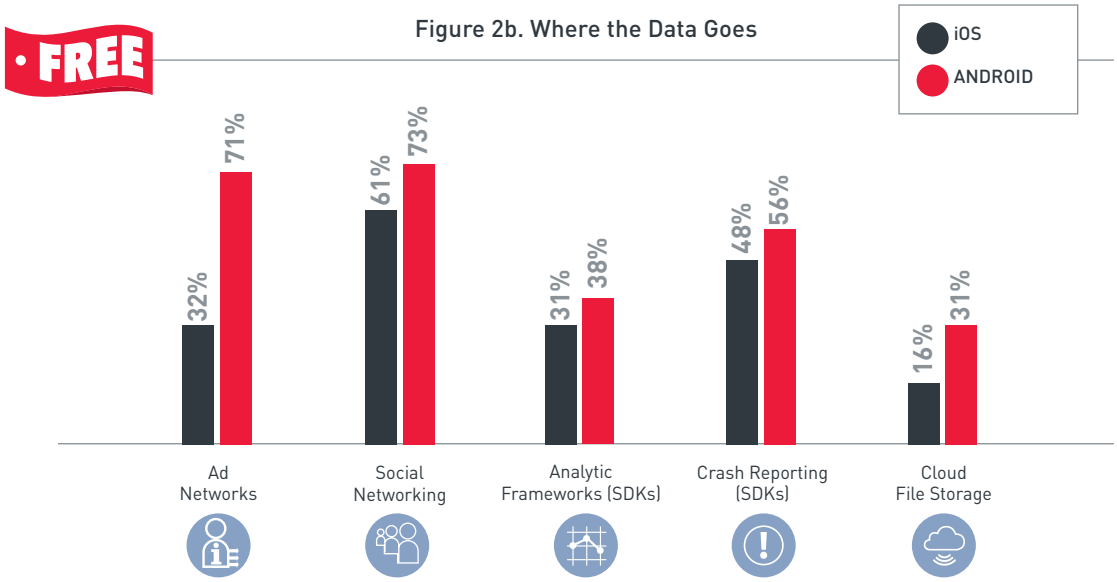
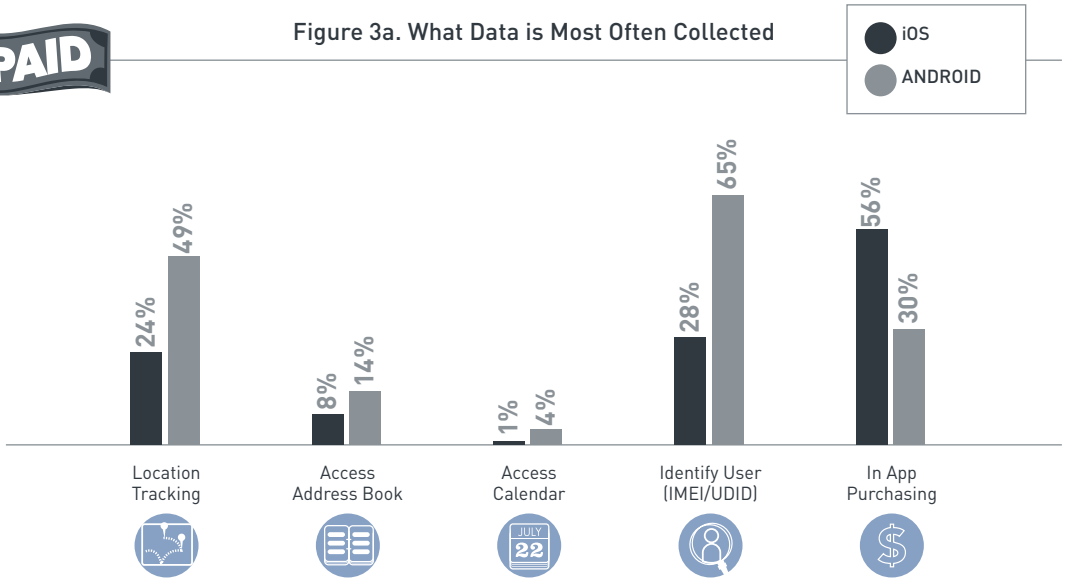


Figure 3. Top 10 Risky Behaviors: Data Collection and Where the Data Goes.

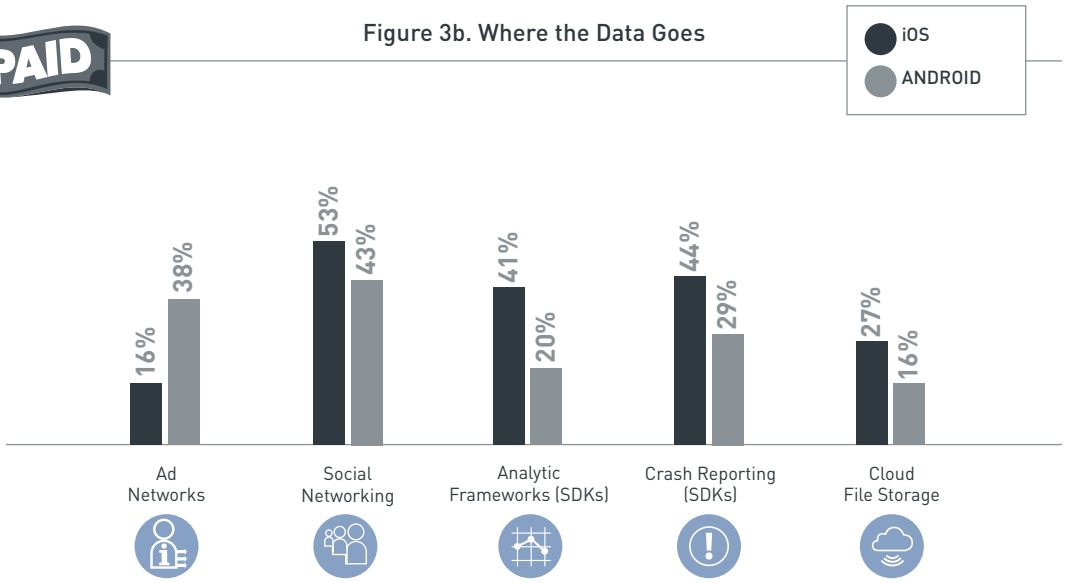
PAID

Figure 3a. What Data is Most Often Collected



PAID

Figure 3b. Where the Data Goes



appthority
TRUST YOUR APPS

What Data Is Most Often Collected?

Tracks User's Location

- 82% of the top Android free apps and 49% of the top Android paid apps track user's location
- 50% of the top iOS free apps and 24% of the top iOS paid apps track user's location

Smartphone users generally understand what location tracking is and are fairly aware of some of the risks associated with carrying a device that knows your location at all times. But, location tracking is being conducted in a lot of different ways, by a lot of different entities. One of the most popular approaches is when a developer embeds a tracking code into an app. One of the main reasons app developers initiate app tracking is to generate supplementary revenue by sharing app user data with advertising networks and analytics companies. In some cases, particularly with free apps, developers are paid based on the amount of data they collect and share about users. To see just how prevelant this is, take a look at the Flashlight or Calculator apps. They request your permission to access your location! Now you know why!

The risk: An app may be able to silently trigger the microphone when a mobile device is in a particular geo-location or track your location at certain times of the day. Beyond the physical security concerns of knowing when you are not home, or where a top executive is traveling, there are also corporate espionage concerns. What if a photo tag reveals that a member of your M&A team is in the hometown of a key competitor?

Accesses User's Address Books

- 30% of the top Android free apps and 14% of the top Android paid apps access user's address books
- 26% of the top iOS free apps and 8% of the top iOS paid apps access user's address books

App developers often collect and transmit the contacts or full address book located on the device. One reason generally relates to increasing the viral or network effects of the app. In other words, the developer wants to use the owner's contacts to expand their customer base. Or another reason may be that the developer has leveraged 3rd party SDKs that include the ability to download a user's address book for the purpose of marketing additional mobile apps or services to those in the contact list.

There are a lot of problems with these approaches. For one, who are the contacts on a device? For instance, if a consumer buys an iPhone and plugs it into his or her corporate desktop at work, it will give them the option to sync with contacts from Outlook. Those Outlook contacts are likely a combination of personal and enterprise contacts, with the enterprise contacts being owned by the organization and possibly not even people the user knows. If the app were to ask for permission to access the address book, it would be the user saying "yes," even though the contacts belong to the enterprise.

The risk: In addition to the privacy concern of sharing personal or corporate contacts, or the potential for corporate espionage and theft of valuable contacts, Appthority has also seen an increase in corporate spam as advertisers get list of corporate phone, email, titles, and physical mail address from corporate address books leaking from devices.

Accesses User's Calendars

- 2% of the top Android free apps and 4% of the top Android paid apps access user's calendars
- 8% of the top iOS free apps and 1% of the top iOS paid apps access user's calendars

Mobile apps that access calendar data have very similar issues as those accessing user's contacts. In both cases there is a high potential for data leakage and the exposure of corporate data. If an app accesses a user's calendar, that app has a window into every line of information stored within that calendar. Users often store the names and phone numbers for meeting attendees, meeting minutes and attachments within the notes section – which could include financial spreadsheets, corporate presentations, and other forms of sensitive data, all accessible via the calendar.

The risk: All the data stored in calendar invites, including meeting minutes, call-in information, call passwords, attachments, folks attending, topics discussed, could lead to corporate espionage. The good news, however, is this behavior has improved over time as apps (like LinkedIn) have gotten in trouble for accessing calendars without permission, providing a good example of developers listening when users fight back for their privacy. As of iOS 7, Apple now asks users for permission before allowing apps to access calendar data, homever a proper enterprise security program should include user education, so employees know when they are allowed to share calendars and when not to.

Tracks Users with IMEI/UDID

- 88% of the top Android free apps and 65% of the top Android paid apps access IMEI/UDID
- 57% of the top iOS free apps and 28% of the top iOS paid apps access IMEI/UDID

Access to UDIDs is a concern because with a unique device identifier, developers can correlate user behavior across multiple apps (even if they have different usernames and passwords for each of the apps) and then match them to a unique user. Developers and ad networks may also match UDIDs to real user data, including names, passwords, locations and other information. While Apple has prohibited iOS developers from using UDIDs as a means to track and identify users, Appthority discovered that the new rule is only enforced on devices which are running the latest version of iOS. Furthermore, Apple has encouraged developers to use new methods of user identification, to track user behavior on an app-by-app basis.

The risk: A UDID or IMEI is like a web-based cookie that you can't delete, so one of the main risks with UDID tracking is the "permanent" nature of the device to user link. The alphanumeric number linked to a unique device allows developers and ad networks to create a complete profile of a user across multiples apps and profiles and combine with other risky behaviors for an in-depth view of the device owners.

Allows for In-app Purchases

- 58% of the top Android free apps and 30% of the top Android paid apps enable in-app purchases
- 55% of the top iOS free apps and 56% of the top iOS paid apps enable in-app purchases

Most app developers struggle to monetize their apps. Users usually opt for free apps or for cheap apps ($0.99). Thus, app developers are incented to integrate in-app purchasing for additional revenue on top of what they gain from the initial download. In-app-purchasing allows consumers to buy a variety of items from within the original app, including other apps, services, additional functionality, premium content, etc.

For users whose carrier allows for carrier billing of in-app purchases, in-app purchasing may be a concern to employees as they may incur unauthorized costs that will appear on an employer's bill. In-app purchasing is also a concern when it comes to apps for children, as they may be able to purchase content within apps without the parent's knowledge… until the bill arrives.

The risk: In-app purchasing is an increasing concern to parents as children may have the ability to make in-app purchases which may be charged to an employer who pays for the monthly usage of a work device. In-app purchases have proved to be controversial, The European Commission recently insisted that Apple and Google no longer label apps which allow for in-app purchases as "free apps." If your corporation reimburses employee cellphone use, make sure your team has developed a policy around in-app purchases.

Where Does the Data Go?

Shares User Data with Ad Networks

- 71% of the top Android free apps and 38% of the top Android paid apps share user data with ad networks
- 32% of the top iOS free apps and 16% of the top iOS paid apps share user data with ad networks

App developers seek out additional ways to generate revenue beyond the price to download, especially when most apps offer a free download. Unfortunately, this comes at a cost to user privacy and security. While developers of paid apps receive part of the initial download fee, free app developers are completely dependent on other revenue streams that might be built into and present within a free app. In addition, developers often continue to support their users with new content and newer versions of the app for free. So how might developers make money after that initial download?

One popular method app developers employ to generate supplementary revenue is through sharing user data with advertising networks and analytics companies. In some cases, developers are paid based on the amount of data they collect and share about users. While sharing data with ad networks is often expected from free apps (how else would developers monetize?), it was surprising to find that a large and growing percentage of paid apps also share data with ad networks. Although the user might not be presented with ads as with the free apps, the app developers share data collected with advertising firms and data brokers behind the scenes.

The risk: All the data collected by risky behaviors can be sold/shared with 3rd party ad networks and data brokers. This data can easily combine both user data and enterprise data that has been grouped together on a single device. Although this behavior was originally primarily seen on free apps, this behavior is now seen on both free and paid apps. Once data leaves the device, it is essentially gone forever. Because sensitive corporate data coexists with personal user data on the device, it is important to monitor app data harvesting and sharing with third parties to prevent corporate data loss.

Shares User Data with Social Networking (allows for single-sign-on with social networking)

- 73% of the top Android free apps and 43% of the top Android paid apps share user data with social networking sites
- 61% of the top iOS free apps and 53% of the top iOS paid apps share user data with social networking sites

Adding to the list of 3rd parties that collect app and user data, social networking integration is one of the fastest growing categories. Single sign-on (SSO) support, where the mobile app enables users to sign in via integration to a social networking site's login (such as Facebook or Twitter), is one of the latest trends in the app ecosystem.

Support for social networking SSO makes for a simplified user experience. However, this behavior is also seen as a risk in a BYOD or Mobile First context, because any data that was previously harvested off a device and shared with ad networks and data brokers, now also makes its way to giant social networking sites (with their own sets of ad networks). Furthermore, if a user's social login is compromised, all of the apps (and websites) that the user has logged into using that same password might be compromised as well.

The risk: Developers have embraced social networking SDKs (software developer kits) that allow their users to log-in to their app with a social network. However, in return (and often unknowingly to the user), social networks gets access to user device and app data that the developer collected. An increase in the number of third parties that get ahold of user's data opens up the potential of misuse. Social networking data sharing also presents several privacy concerns, as user data previously collected by the social network now also becomes available to the app developer and the ad networks built into the app itself.

Shares Data with 3rd Party Analytic Frameworks

- 38% of the top Android free apps and 20% of the top Android paid apps share user data with 3rd Party Analytic Frameworks
- 31% of the top iOS free apps and 41% of the top iOS paid apps share user data with 3rd Party Analytic Frameworks

Many developers use off-the-shelf, 3rd party tools–such as software developer kits (SDKs) and libraries. This approach allows programmers to develop apps faster and more efficiently, leveraging third-party functionality, and tapping into aggregate data only available through a "network effect". A great risk in using SDKs and/or third-party code is that a developer may unwittingly introduce undesirable behaviors into his/her own apps. Some of the most popular SDKs are analytics frameworks, which collect a plethora of user and app usage metrics across the developer's app, and millions of other apps, to give the developer incredible depth of information on user mobile engagement across their app and the app ecosystem. Analytics frameworks are yet another 3rd party to worry about that is aggregating, sorting, and deeply analyzing user and app data, increasing the complexity of answering the question "where could my sensitive data end up?"

The risk: Similar to sharing data with social networks, many SDKs share data with 3rd party analytics frameworks like Flurry Analytics & Google Analytics, which in turn provide analytics services to the developers to track the use of their app. However developers, and the analytics companies themselves, can then resell this data to advertisers and data brokers.

Shares User and App Data with 3rd Party Crash Reporting

- 56% of the top Android free apps and 29% of the top Android paid apps share user and app data with 3rd party crash reporting
- 48% of the top iOS free apps and 44% of the top iOS paid apps share user and app data with 3rd party crash reporting

As competition stiffens and developers struggle to stay in their users' list of favorite apps, app performance and functionality become critical. Increasingly, developers are turning to 3rd parties to help monitor app performance, and as a result, there has been a boom of 3rd party Crash Reporting SDKs making their way into the top iOS and

Android apps. While these 3rd parties are definitely less risky than their advertising, social networking, and analytic counterparts (mostly because they are focusing on app performance, crashes, and bugs), this practice may be risky as it increases the number of 3rd parties receiving data harvested from the device, as well as it introduces 3rd party code into a developer's own app. Introducing 3rd party code can result in unknown security issues and unknown app behaviors.

The risk: Although less risky than the other 3rd party SDKs mentioned previously in the report, Crash Reporting SDKs are yet another 3rd party collecting user (and sometimes corporate) device data and introducing foreign code into a developer's app. However, there are risks in the way that most crash reporting services work. When an app crashes, app data and crash logs are sent to the crash reporting service for analysis. The crash logs often include confidential data that the user typed into the app and are sometimes even shared without encryption.

Allows Users to Save data/files on Public Cloud File Storage Providers

- 31% of the top Android free apps and 16% of the top Android paid apps allow users to save data on public cloud file storage providers
- 16% of the top iOS free apps and 27% of the top iOS paid apps allow users to save data on public cloud file storage providers

As more users move their data to the cloud, app developers have jumped on the cloud-storage bandwagon and are increasingly including back-end connections to popular public cloud storage solutions directly into their apps. While this trend makes it easier for consumers to share and store data publicly, it creates a nightmare scenario for corporations who want to limit the amount of confidential files that end up on public cloud due to "Rogue IT". Although some companies have implemented policies to ban the use of public cloud apps like Box or Dropbox, even if these apps are blocked, there are now thousands of apps that can save files directly to Box and Dropbox through the use of SDKs and APIs built into apps. For example, even without the Dropbox app present on a device, a user may now save files directly to Dropbox from a number of the top iOS and Android apps.

The risk: The enterprise is trying to stop the "Rogue IT" phenomenon specifically as it applies to corporate documents making their way into the public cloud. Although some corporations are looking to block access to a specific public cloud app like Dropbox, this approach is unsuccessful as more and more apps have direct access to this and other public cloud storage providers. App risk management solutions are crucial to look for risky app behaviors, not just app categories or app names, to identify and remediate against corporate risk.

Risky Behaviors of Paid vs. Free Apps

Are Paid Apps Safer Than Free Apps?

By a large margin, free apps are riskier than paid apps. The biggest disparity between free and paid apps is location tracking. While 66% of free apps track for location, less than half of paid apps (37%) do the same. Free apps are also more likely than paid apps to use single sign-on (67%), share data with ad networks (52%) and analytic frameworks (35%), offer in-app purchasing (57%), identify the user or UDID (73%), and access the address book or contact list (28%).

Paid apps, on the other hand, aren't nearly as safe as one might think. While 99% of free apps exhibited at least one risky behavior, so did 83% of the top paid apps. Developers of paid and free apps are seeking new methods of generating revenue and unfortunately, it comes at the cost of the user's privacy.

Paid apps trailed free apps across all types of risky behaviors:

- In-app purchasing (43%)
- Single sign-on (48%)
- Sharing with ad networks (27%)
- Sharing data with analytic frameworks (31%)
- Identifying the user or UDID (47%)
- Accessing the address book or contact list (11%)
- Accessing the calendar (3%)

Risky Behaviors of iOS vs. Android Apps

When comparing the top iOS and Android apps (both paid and free), iOS apps exhibited a greater percentage of risky behaviors than Android apps did. Appthority determined that 93% of iOS apps exhibit at least one risky behavior mentioned in this report, as compared to 89% of Android apps.

Of the 200 iOS apps the Appthority App Risk Management Service tested (100 free, 100 paid), 37% tracked for location, 57% used single sign-on, 56% offered in-app purchasing, 24% shared data with ad networks, 36% shared data with analytic frameworks, 17% accessed the address book or contact list, and 5% accessed the calendar.

There was one behavior that Android apps exhibit significantly more than iOS apps; more Android apps access the UDID, 77% of the top 200 to identify the user from that information. Apple actually discourages iOS developers from accessing UDIDs, but the Appthority Service identified that 43% of the top iOS apps are still trying to access the UDID this, which is actually 37 percentage points higher than the findings in Appthority's Summer 2013 report.

While Android apps exhibited fewer risky behaviors overall, they weren't far behind iOS apps. From the 200 free and paid Android apps Appthority tested, 66% tracked for location, 58% used single sign-on, 55% apps shared data with ad networks, 29% shared data with analytic frameworks, 44% supported in-app purchasing, 77% identified the user (or UDID), 22% accessed the contact list or address book, and 3% accessed the user's calendar.

iOS Apps: Paid vs. Free

Apple iPhone and iPad users should note that free iOS apps are riskier than paid iOS apps on the whole, except for in-app purchasing, and accessing cloud file storage and analytic frameworks.

In testing the top 100 free iOS apps, Appthority determined that 50% tracked for location, 61% used single sign-on, 55% offered in-app purchasing, 26% accessed the user's contact list or address book, 32% shared data with advertising networks, 31% share data with or analytic frameworks, 8% accessed the user's calendar and 57% identified the user or UDID.

However, more paid iOS apps (56%) supported in-app purchasing over free iOS apps (55%). This is interesting because paid apps already generate revenue when first downloaded. A significant percentage of paid apps also share data with advertising networks (16%) and analytic frameworks (41%), which is a common method of monetization as well. Additionally, more paid iOS apps access cloud file storage (27%) vs. free iOS apps (16%)

Other risky behaviors present in the top 100 paid iOS apps include using single sign-on (53%), location tracking (24%), and identifying the user or UDID (28%).

Android Apps: Paid vs. Free

Appthority determined that free Android apps exhibit more risky behaviors than paid Android apps overall, except when it comes to accessing the user's calendar. Significant percentages of both free and paid Android apps identify the user or UDID — far more than iOS apps.

In testing the top 100 free Android apps, the Appthority Service found that 88% identify the user or UDID, 82% track for location, 73% use single sign-on, 71% share data with ad networks, 38% share data with analytic frameworks, 58% support in-app purchasing, 30% access the contact list or address book, and 2% access the calendar.

Of the top 100 paid Android apps, 65% identify the user or UDID, 49% track for location, 30% offer in-app purchasing, 43% use single sign-on, 38% share data with ad networks, 20% share data with analytic frameworks, 14% access the contact list or address book, and 4% access the calendar.

So... Free vs Paid?

In a BYOD or Mobile First context, IT cannot simply suggest that employees use paid apps over free apps. Appthority revealed that although free apps do pose a greater risk to their paid counterparts, there were enough risky behaviors present in paid apps to cause concern as well. An App Risk Management solution needs to be in place in order to be able to analyze all apps (free & paid) at scale.

Developer Breakdown

From the 400 tested apps, the Appthority App Risk Management Service identified the key developers behind the most popular mobile apps. The charts below feature developers that have two or more apps in the top 100 free or paid apps in the Apple App Store or Google Play Store.

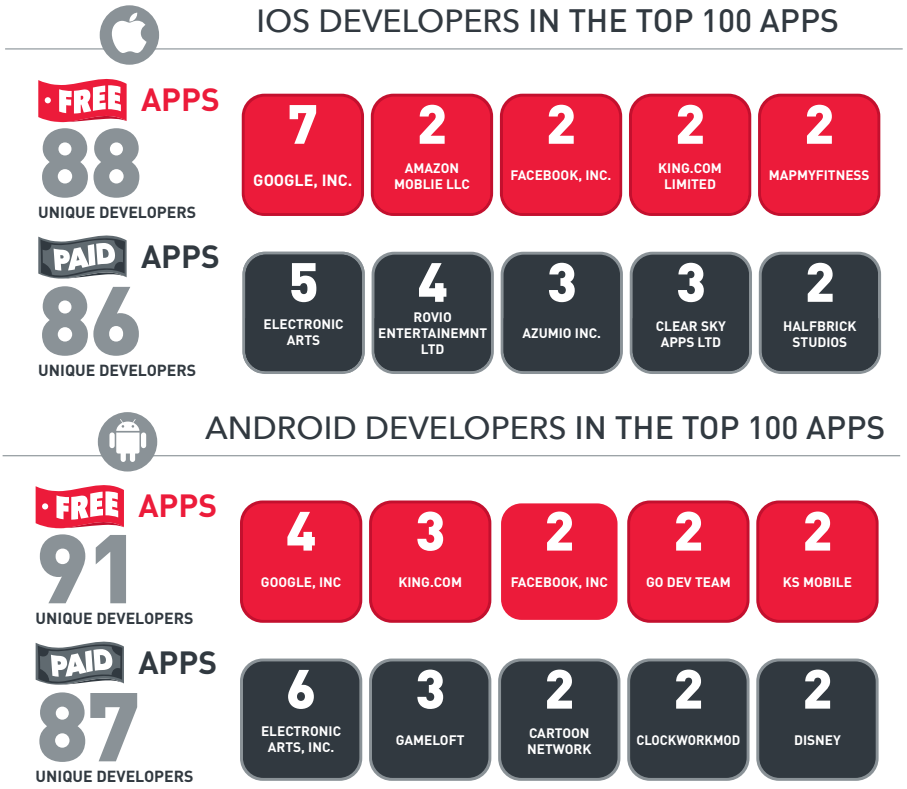
Ironically, Google, Inc. dominated the market share of popular iOS free apps (7 apps in the top 100), followed by Amazon (2 apps), Facebook (2 apps), King.com (2 apps) and a few others. There were 88 different developers in the top 100 free iOS apps, with only 7 developers who had more than 1 app in the top 100 free apps.

For iOS paid apps, gaming giants Electronic Arts (5 apps in the top 100) and Rovio Entertainment (4 apps) dominated the landscape, followed by Azumio Inc. (3 apps), and Clear Sky Apps (3 apps). There were 86 different developers in the top 100 paid iOS apps, whith only 7 developers who had more than 1 app in the top 100 paid apps.

On the Android free side, Google, Inc. led the pack (4 apps), followed by King.com (3 apps), Facebook (2 apps), and others. There were 91 different developers in the top 100 free Android apps, and only six developers had more than one app in the top 100 free Android apps.

For the top 100 paid Android apps, there were 87 different developers. As with iOS paid, game developers lead the pack, in this case Electronic Arts (6 apps) and Gameloft (3 apps), followed by Cartoon Netwrok (2 apps), Disney (2 apps), and others. Only 8 developers had more than 1 app in the top 100 Android paid apps.

Figure 4. Who's Who - Developers in the Top 100



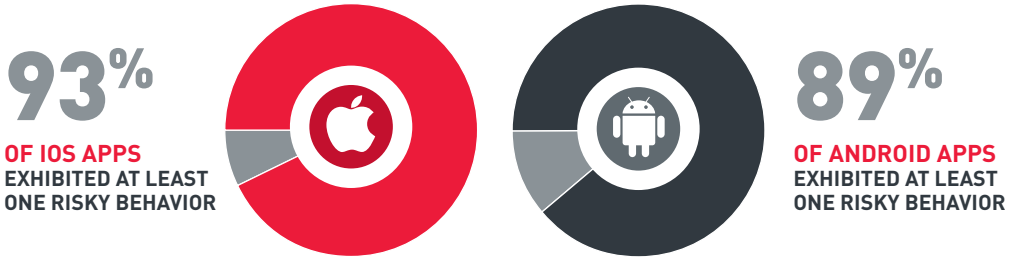
In a BYOD or Mobile First context, the sheer number of individual developers makes for a big headache for IT. IT professionals must adopt new methods to manage the massive number of apps (from all types of developers) that are entering the workplace on employee devices. Gone are the days where software came into the enterprise from a few, trusted developers. In today's Bring Your Own App (BYOA) environment, mobile apps come into corporate environments from developers large and small from all over the world.

Summary and Analysis

The results of the Appthority Summer 2014 App Reputation Report confirms that app risky behaviors continue to rise, particularly for free apps on both platforms (99% of free apps demonstrated at least one of the Top 10 risky behaviors). While paid apps are less risky than free apps, users are by no means protected by only downloading paid apps. Appthority found that 83% of the top paid apps exhibited at least one risky app behavior. It's clear that app business models are focusing on collecting user data (and in many cases, selling that data) regardless of whether users have paid for an app or not. In Mobile First, BYOD and BYOA, user data and corporate data live together on the device, making privacy and security concerns relevant to both the users and IT departments.

While Apple's mobile ecosystem is often considered safer in comparison to Android's "open" platform, that's not always the case in terms of apps' hunger for user data. Overall, 93% of iOS apps exhibited at least one risky behavior, as compared to 89% of Android apps.

Figure 5. Risky Behaviors – iOS vs. Android.



Additionally, the Appthority Service discovered that 43% of the most popular iOS apps are still trying to access UDIDs to identify and track users, even though Apple explicitly discourages that activity. This makes one wonder what else Apple might be missing during their app review process.

In summary, the only way to avoid security and privacy problems is to have access to real-time deep dynamic and behavior analysis of mobile app risk and be able to apply customized policies to limit use of the riskiest apps.

Organizations adopting Mobile First, BYOD, and Bring Your Own Apps policies that want to prevent security and corporate privacy risks, such as location tracking of executives or the leaking of sensitive corporate data, need to incorporate automated App Risk Management. Only by comprehensive visibility into the risky behaviors hidden within mobile apps can organizations build stronger defenses against current and future threats and fully leverage the potential of mobility to empower a safe and secure mobile workforce.

appthority
TRUST YOUR APPS

Counts for iOS FREE, and App Developer

1. 2048 ..... Ketchapp
2. 100 Balls ..... Giedrius Talzunas
3. 2048 plus - Challenge Edition..... redBit games
4. 8 Ball Pool™..... Miniclip.com
5. Amazon App ..... AMZN Mobile LLC
6. Angry Birds Go!..... Rovio Entertainment Ltd
7. AutoRap by Smule..... Smule
8. Badoo - Meet New People, Chat, Socialize..... Badoo Software Ltd
9. Bank of America ..... Bank of America
10. Bible ..... LifeChurch.tv
11. Boom Beach..... Supercell
12. Candy Crush Saga..... King.com Limited
13. CastleStorm - Free to Siege ..... ZEN Studios Ltd.
14. Chase Mobile..... JPMorgan Chase & Co
15. Chrome - web browser by Google .. Google, Inc.
16. Clash of Clans..... Supercell
17. CSI: Hidden Crimes..... Ubisoft
18. Despicable Me: Minion Rush ..... Gameloft
19. dEXTRIS..... Chaotic Box
20. Don't step the white tile..... Ayumu Kinoshita
21. Don't Tap The White Tile 2 ..... WANG BOXUN
22. Dont touch the white tile..... Lucky Studio
23. Dropbox..... Dropbox
24. eBay..... eBay Inc.
25. Emoji→ ..... Emoji+
26. ESPN FC Soccer & World Cup ..... ESPN
27. Expedia Hotels & Flights ..... Expedia, Inc.
28. Facebook..... Facebook, Inc.
29. Facebook Messenger..... Facebook, Inc.
30. Farm Heroes Saga ..... King.com Limited
31. FarmVille 2: Country Escape ..... Zynga Inc.
32. Flappy Bird: New Season..... Dong Nguyen
33. Flappy Smash - The End of a Tiny Bird..... Makeover Mania Story Games
34. Flipagram..... Cheerful, Inc.
35. Free Video Downloader Plus -- ..... zhou Xingfa Download HD video and enjoy it right away
36. Frozen Free Fall..... Disney
37. Gmail - email from Google ..... Google, Inc.
38. Google Docs ..... Google, Inc.
39. Google Drive..... Google, Inc.
40. Google Maps..... Google, Inc.
41. Google Search..... Google, Inc.
42. Groupon..... Groupon, Inc.
43. Hotels.com – Hotel Booking..... Hotels.com and last minute hotel deals
44. Hungry Shark Evolution..... Future Games of London
45. iHeartRadio – Free Music &..... Clear Channel Management Internet AM/FM Radio Stations Services, LP
46. Impossible Flappy - Flappy's Back . EmBraze
47. InstaCollage Pro - Pic Frame & Photo Collage & Caption Editor for Instagram FREE..... click2mobile
48. Instagram..... Instagram, Inc.
49. InstaSize - Post Entire Photos..... Munkee Apps L.L.C. On Instagram Without Cropping
50. iTube - Playlist Management..... Shiri Markish
51. Job Search ..... Indeed.com
52. Kik Messenger ..... Kik Interactive Inc.
53. Kindle ..... AMZN Mobile LLC
54. LINE..... NAVER JAPAN
55. LinkedIn ..... LinkedIn Corporation
56. Litely..... Litely LLC
57. Magic Piano by Smule..... Smule
58. Make It Rain: The Love of Money.... Space Inch, LLC
59. MLB Big Stars Baseball..... Hothead Games Inc.
60. MLB Perfect Inning..... GAMEVIL USA, Inc.
61. myAT&T..... AT&T Services, Inc.
62. Netflix..... Netflix, Inc.
63. Pandora Radio..... Pandora Media, Inc.
64. PayPal ..... PayPal Inc
65. Perfect365 - One-Tap Makeover..... ArcSoft, Inc.
66. Piano Tiles..... HU WEN ZENG
67. Pic Stitch ..... Big Blue Clip, LLC
68. Pinterest..... Pinterest, Inc.
69. Real Estate by Zillow..... Zillow.com
70. Run with Map My Run - ..... MapMyFitness GPS Running, Jog, Walk, Workout Tracking and Calorie Counter
71. RunKeeper ..... FitnessKeeper, Inc
72. Shadow Fight 2..... Nekki
73. Shazam..... Shazam Entertainment Ltd.
74. Skype for iPhone ..... Skype Communications S.a.r.l
75. Smash Hit..... Mediocre AB
76. SoundCloud: stream music &..... SoundCloud Ltd. audio and listen to playlists
77. Spotify Music..... Spotify Ltd.
78. Tango Text, Voice & Video ..... TangoMe, Inc.
79. The Sims™ FreePlay..... Electronic Arts
80. The Weather Channel and ..... The Weather Channel Interactive weather.com - local forecasts, radar, and storm tracking
81. Timehop ..... Timehop
82. Toilet Time - Mini Games..... Tapps Tecnologia da to Play in the Bathroom InformaÃ§Ã£o Ltda.
83. TripAdvisor ..... TripAdvisor LLC
84. Tumblr..... Tumblr
85. Twitter ..... Twitter, Inc.
86. Uber..... Uber Technologies, Inc.
87. Unroll Me - unblock the slots..... Turbo Chilli Pty Ltd
88. Viber ..... Viber Media, Inc.
89. Viggle..... Viggle, Inc.
90. Walgreens ..... Walgreen Co
91. Walk with Map My Walk ..... MapMyFitness
92. WeatherBug ..... Earth Networks, Inc
93. Weed Firm..... Manitoba Games
94. Wells Fargo Mobile ..... Wells Fargo
95. What's the Difference? ~ spot..... Candywriter, LLC the differences & hidden objects in this photo puzzle hunt!
96. Wish - Shopping Made Fun..... ContextLogic Inc.
97. Yahoo Mail – Free Email App ..... Yahoo
98. Yelp..... Yelp
99. YouTube ..... Google, Inc.
100. Zombie Road Trip Trials..... Noodlecake Studios Inc

appthority
TRUST YOUR APPS

Counts for iOS PAID and App Developer

1. 10K Runner ..... Clear Sky Apps LTD
2. 1Password - Password Manager and Secure Wallet .... AgileBits Inc
3. 2-bit Cowboy ..... Crescent Moon Games
4. 5K Runner ..... Clear Sky Apps LTD
5. 8mm Vintage Camera ..... Nexvio Inc.
6. Age of Zombies ..... Halfbrick Studios
7. Akinator the Genie ..... Elokence
8. Angry Birds ..... Rovio Entertainment Ltd
9. Angry Birds Seasons..... Rovio Entertainment Ltd
10. Angry Birds Star Wars ..... Rovio Entertainment Ltd
11. Backflip Madness..... Gamesoul Studio
12. Bad Piggies ..... Rovio Entertainment Ltd
13. Bloons TD 5..... Ninja Kiwi
14. CamCard ..... IntSig Information Co.,Ltd
15. Camera+..... tap tap tap
16. CamScanner + PDF Document..... IntSig Information Co.,Ltd
17. Couch-to-5k..... The Active Network, Inc.
18. Cut the Rope ..... Chillingo Ltd
19. Cut the Rope 2..... ZeptoLab UK Limited
20. Daily for Craigslist ..... Lifelike Apps, Inc
21. Dark Sky..... Jackadam
22. Duck Life ..... MoFunZone Inc
23. Dude Perfect ..... Dude Perfect
24. Earn to Die ..... Not Doppler
25. Emoji ;) ..... Emoji+
26. Facetune..... Lightricks Ltd.
27. Fitness Buddy ..... Azumio Inc.
28. Flick Home Run! ..... infinity pocket
29. Flightradar24 Pro..... Flightradar24 AB
30. Fruit Ninja ..... Halfbrick Studios
31. Full Fitness: Exercise Workout Trainer..... Mehrdad Mehrain
32. Geometry Dash ..... Robert Topala
33. Grand Theft Auto: San Andreas ..... Rockstar Games
34. Heads Up!..... Warner Bros.
35. HotSchedules..... HotSchedules
36. InstaCollage Pro click2mobile
37. Instant Heart Rate..... Azumio Inc.
38. iTrackBites ..... Ellisapps Inc.
39. Jesus Calling Devotional by Sarah Young..... Nelson Media, Inc.
40. Kick the Buddy: No Mercy..... Crustalli
41. Leo's Fortune ..... 1337 & Senri LLC
42. Lock Screen Plus ..... Faizan Kasbati
43. Lockscreen Factory - Wallpapers for iOS 7 ..... Abdel Satar Mahmoud
44. Mail+ for Outlook..... iKonic Apps LLC
45. Make Emoji Pro for iOS 7 ..... Valerie Fehringer
46. Map My Ride+..... MapMyFitness
47. Mickey Mouse Clubhouse: Mickey's Wildlife Count Along ..... Disney
48. MotionX GPS Drive ..... MotionXâ„¢
49. My Talking Pet..... WOBA Media
50. Omegle ..... Omegle.com LLC
51. On the line ..... Kevin Choteau
52. Over ..... Potluck
53. P90X ..... Beachbody, LLC
54. Papa's Burgeria To Go! ..... Flipline Studios
55. Period Tracker Deluxe ..... GP Apps
56. PhotoToaster..... East Coast Pixels, Inc.
57. PicFrame..... ActiveDevelopment
58. Plague Inc ..... Ndemic Creations
59. Plants vs. Zombies..... PopCap
60. Plex..... Plex Inc.
61. Pou ..... Paul Salameh
62. Runtastic PRO ..... runtastic
63. Scan - QR Code and Barcode Reader ..... QR Code City
64. Scanner Pro ..... Readdle
65. Scribblenauts Remix..... Warner Bros.
66. Simply Being ..... Meditation Oasis
67. Sky Tourist..... Full Phoenix
68. Sleep Cycle alarm clock..... Azumio Inc.
69. Sleep Pillow Sounds ..... Clear Sky Apps LTD
70. Smart Alarm Clock ..... Plus Sports
71. Spotipremeir for Spotify Premium..... Rose King
72. Stack the States ..... Freecloud Design, Inc.
73. Star Rover ..... EEFan Inc.
74. Storm Shield ..... E.W. Scripps Company
75. Superimpose..... Pankaj Goswami
76. Survivalcraft ..... Igor Kalicinski
77. Terraria ..... 505 Games (US), Inc.
78. Tetris ..... Electronic Arts
79. The Game of Life..... Electronic Arts
80. The Impossible Game ..... FlukeDude Ltd
81. The Room Two..... Fireproof Games
82. The Sims 3..... Electronic Arts
83. The Sims 3 Ambitions ..... Electronic Arts
84. The Wonder Weeks ..... Domus Technica
85. Threes! ..... Sirvo LLC
86. Tiger Woods PGA Tour 12 ..... Electronic Arts
87. Tiny Wings..... Andreas Illiger
88. TinyScan Pro ..... Appxy
89. Toca Hair Salon 2 ..... Toca Boca AB
90. True Skate..... True Axis
91. TurboScan ..... Piksoft Inc.
92. Ultimate Guitar Tabs..... Ultimate Guitar
93. Video Shop - Video Editor ..... Joseph Riquelme
94. Waterlogue..... Tinrocket, LLC
95. Wheel of Fortune ..... Sony Pictures Television
96. Wipeout ..... Activision Publishing, Inc.
97. WolframAlpha ..... Wolfram Group LLC
98. Yoga Studio..... Modern Lotus
99. Zombie Highway..... Auxbrain, Inc.
100. Zombies, Run!..... Six to Start

appthority
TRUST YOUR APPS

Counts for Android FREE and App Developer.

1. 2048 Number puzzle game ..... Estoty Entertainment Lab
2. Adobe Reader ..... Adobe Systems
3. Amazon ..... Amazon Mobile LLC
4. Angry Birds ..... Rovio Mobile Ltd.
5. Bank of America ..... Bank of America
6. Battery Doctor (Battery Saver) ..... KS Mobile
7. Bible ..... LifeChurch.tv
8. Big Fish Casino - Free SLOTS ..... Big Fish Games
9. Bingo Fever - Free Bingo Game ..... TOPFUN
10. Blooming Night Keyboard Theme ... GO Dev Team
11. Calorie Counter - MyFitnessPal ..... MyFitnessPal, Inc.
12. Candy Blast Mania ..... TeamLava Games
13. Candy Crush Saga ..... King.com
14. Castle Clash ..... IGG.COM
15. Cats & Dogs Casino -FREE Slots .... Gamelion Studios
16. Chase Mobile ..... JPMorgan Chase
17. Clash of Clans ..... Supercell
18. Clean Master - Free Optimizer ..... KS Mobile
19. Coin Dozer - Free Prizes! ..... Game Circus LLC
20. CSI: Hidden Crimes ..... Ubisoft Entertainment
21. DEER HUNTER 2014 ..... Glu
22. Despicable Me ..... Gameloft
23. Don't Tap The White Tile ..... HU WEN ZENG
24. Dropbox ..... Dropbox, Inc.
25. eBay ..... eBay Mobile
26. Emoji Keyboard - Emoticons(KK) ... Kaka Mobile
27. Facebook ..... Facebook
28. Facebook Messenger ..... Facebook
29. Family Guy The Quest for Stuff ..... TinyCo
30. Farm Heroes Saga ..... King.com
31. Flipagram ..... Flipagram, inc.
32. Flow Free ..... Big Duck Games LLC
33. Forest Mania™ ..... yang suhongs
34. Fruit Ninja Free ..... Halfbrick Studios
35. Game of War - Fire Age ..... Machine Zone, Inc.
36. Glide - Video Texting ..... GlideâĐ‰
37. GO SMS Pro ..... GO Dev Team
38. Google Docs ..... Google Inc.
39. Google Earth ..... Google
40. Google Sheets ..... Google Inc.
41. Google Translate ..... Google Inc.
42. Groupon - Daily Deals, Coupons ..... Groupon, Inc.
43. Guess The Emoji ..... Random Logic Games
44. HellFire: The Summoning ..... Mobage
45. Hill Climb Racing ..... Fingersoft
46. iHeartRadio – Internet Radio ..... Clear Channel Broadcasting, Inc.
47. Instagram ..... Instagram
48. Iron Force ..... Chillingo
49. Kik ..... Kik Interactive
50. LINE: Free Calls & Messages ..... LINE Corporation
51. Lost Bubble - Bubble Shooter ..... Peak Games
52. Magic Piano by Smule ..... Smule
53. Make It Rain: Love of Money ..... Space Inch, LLC
54. MLB Perfect Inning ..... GAMEVIL Inc.
55. Monster World HD ..... TeebikGames
56. My Talking Tom Outfit7
57. Netflix ..... Netflix, Inc.
58. ooVoo Video Call, Text & Voice ..... ooVoo LLC
59. Pandora® internet radio ..... Pandora
60. Paperama ..... FDG Entertainment GmbH & Co.KG
61. Pet Rescue Saga ..... King.com
62. Photo GridÐCollage Maker ..... RoidApp
63. PicsArt - Photo Studio ..... PicsArt
64. Pinterest ..... Pinterest, Inc.
65. Plague Inc. ..... Miniclip.com
66. Pou ..... Zakeh
67. Powerboat Racing 3D ..... Doodle Mobile Ltd.
68. Reign of Summoners 2014 ..... Free Card Games
69. Shazam ..... Shazam Entertainment Limited
70. Skype - free IM & video calls ..... Skype
71. Slot Galaxy HD Slot Machines ..... Tap Slots
72. Slots - myVEGAS Slot Machines ..... PlayStudios
73. Slots Fever - Free Slots ..... Kakapo
74. Slots Oz™ - slot machines ..... GORDON ROBINSON
75. Snapchat ..... Snapchat, Inc.
76. Solitaire ..... MobilityWare
77. SoundCloud - Music & Audio ..... SoundCloud
78. Spotify ..... Spotify Ltd.
79. Stickman Basketball ..... Djinnworks e.U.
80. Subway Surfers ..... Kiloo
81. Super-Bright LED Flashlight ..... Surpax Technology Inc.
82. Tango Messenger, Video & Calls .... Tango
83. Temple Run 2 ..... Imangi Studios
84. The Gate - Free RTS CCG game ..... Mobage
85. The Weather Channel ..... The Weather Channel
86. Tumblr ..... Tumblr, Inc.
87. TuneIn Radio ..... TuneIn Inc
88. Twitter ..... Twitter, Inc.
89. Viber ..... Viber Media S.Ã r.l.
90. Vine ..... Vine Labs, Inc.
91. Walgreens ..... Walgreen Co.
92. WatchESPN ..... ESPN Inc
93. WeatherBug ..... Earth Networks
94. Wells Fargo Mobile ..... Wells Fargo Mobile
95. WhatsApp Messenger ..... WhatsApp Inc.
96. Words With Friends Free ..... Zynga
97. World Series of Poker – WSOP ..... Playtika
98. Worldcraft 2 ..... slabs
99. Yahoo Mail – Free Email App ..... Yahoo
100. ZEDGE™ Ringtones & Wallpapers .. Zedge

appthority

Counts for Android PAID and App Developer

1. (Paid)GcnBible A7 ..... GCN(Global Communication Network)
2. AccuWeather Platinum ..... Accuweather.com
3. ai.type Keyboard Plus ..... A.I.type
4. AirSync: iTunes Sync & AirPlay ..... doubleTwist â„¢
5. AllCast Premium..... ClockworkMod
6. Beautiful Widgets Pro..... LevelUp Studio
7. Bloons TD 5 ..... ninja kiwi
8. Business Calendar Pro ..... Appgenix Software
9. Camera ZOOM FX Premium..... androidslide
10. Card Wars - Adventure Time ..... Cartoon Network
11. Chaozhuyin(Paid Version) ..... Chih Chao Yu
12. Couch-to-5K..... ACTIVE Network, LLC
13. Cut the Rope ..... ZeptoLab
14. Docs To Go Premium Key ..... DataViz, Inc.
15. Endomondo Sports Tracker PRO.... Endomondo.com
16. ePSXe for Android ..... epsxe software s.l.
17. Equalizer MusicPlayer(Pay)..... NIMBLESOFT LTD.
18. Exchange by TouchDown Key ..... NitroDesk, Inc.
19. ezPDF Reader - Multimedia PDF ... Unidocs Inc.
20. FoxFi Key (supports PdaNet) ..... FoxFi Service
21. FPse for android..... Schtruck & LDchen
22. Fruit Ninja ..... Halfbrick Studios
23. Gangstar Vegas ..... Gameloft
24. Geocaching..... Groundspeak Inc.
25. Geometry Dash ..... RobTop Games
26. GO Launcher Prime ..... GO Launcher Dev Team
27. Grand Theft Auto III..... Rockstar Games, Inc.
28. Grand Theft Auto: San Andreas ..... Rockstar Games, Inc.
29. Greenify (Donation Package) ..... Oasis Feng
30. HD Widgets ..... cloud.tv
31. Hitman GO..... SQUARE ENIX Ltd
32. HotSchedules..... HotSchedules
33. Icebreaker: A Viking Voyage..... Nitrome
34. IP Cam Viewer Pro ..... Robert Chou
35. iSyncr for iTunes to Android ..... JRTStudio
36. Justin.tv..... Justin.tv, Inc.
37. Machinarium..... Amanita Design
38. Minecraft - Pocket Edition ..... Mojang
39. Modern Combat 4: Zero Hour..... Gameloft
40. MONOPOLY..... Electronic Arts Inc
41. Monsters Ate My Birthday Cake ..... Cartoon Network
42. Moon+ Reader Pro ..... Moon+
43. MX Player Pro ..... J2 Interactive
44. My Backup Pro ..... Rerware, LLC
45. NBA JAM by EA SPORTS™..... Electronic Arts Inc
46. Need for Speed™ Most Wanted ..... Electronic Arts Inc
47. Next Launcher 3D Shell..... GO Launcher Dev Team
48. OfficeSuite 7 Pro (PDF&Fonts) ..... Mobile Systems, Inc.
49. Osmos HD ..... Hemisphere Games
50. Phase 10..... Magmic Inc
51. Plants vs. Zombies..... Electronic Arts Inc
52. PlayerPro Music Player ..... BlastOn LLC
53. Plex for Android ..... Plex, Inc.
54. Pocket Casts ..... shiftyjelly
55. Poweramp Full Version Unlocker... Max MP
56. ProtectedSMS - Paid..... Protected Mobility LLC
57. R.B.I. Baseball 14..... MLB Advanced Media, L.P.
58. ROM Manager (Premium)..... ClockworkMod
59. ROM Toolbox Pro..... JRummy Apps Inc.
60. Root Explorer (File Manager)..... Speed Software
61. Scanner Radio Pro ..... Gordon Edwards
62. SD Maid Pro - Unlocker ..... darken
63. SetCPU for Root Users ..... MichaelHuang
64. Shazam Encore ..... Shazam Entertainment Limited
65. SketchBook Pro ..... Autodesk Inc.
66. Sleep as Android Unlock..... Urbandroid Team
67. Sleep Cycle alarm clock..... Northcube AB
68. SlingPlayer for Phones ..... Sling Media Inc.
69. Smart Lottery (Paid)..... xrHome
70. Smart Tools..... Smart Tools co.
71. SoundHound..... SoundHound Inc.
72. SpongeBob Moves In..... Nickelodeon
73. Stargazer Paid..... FINIK LABS LLC
74. SuperGNES (SNES Emulator)..... Neutron Emulation
75. Survivalcraft..... Candy Rufus Games
76. Swype Keyboard..... Nuance Communications, Inc
77. Tasker..... Crafty Apps EU
78. Taxmann Paid..... TAXMANN
79. Temple Run: Oz..... Disney
80. Terraria. ..... 505 Games Srl
81. The Amazing Spider-Man 2 ..... Gameloft
82. THE GAME OF LIFE..... Electronic Arts Inc
83. The Room..... Fireproof Games
84. The Room Two..... Fireproof Games
85. The Sims™ 3 ..... Electronic Arts Inc
86. Threes! ..... Sirvo llc
87. Topia World Builder ..... Crescent Moon Games
88. Torque Pro (OBD 2 & Car)..... Ian Hawkins
89. Trickster MOD Donate Key..... Team Trickster
90. True Skate ..... True Axis
91. tTorrent - Torrent Client App ..... 3D Magic LLC.
92. TuneIn Radio Pro..... TuneIn
93. Ultimate Guitar Tabs & Chords..... Ultimate Guitar USA LLC
94. Where's My Water? ..... Disney
95. Wipeout ..... Activision Publishing, Inc.
96. WolframAlpha ..... Wolfram Alpha, LLC
97. World of Goo..... 2D BOY
98. Worms 2: Armageddon ..... Team 17 Digital Limited
99. XDA Premium..... xda-developers
100. Zooper Widget Pro ..... MYCOLORSCREEN

About Appthority

Appthority's Mobile App Risk Management service automates the discovery, analysis, and approval of apps present on employee devices. Only Appthority combines the largest global database of millions of previously analyzed public and enterprise apps with a policy management engine to automate app review and approval of new apps as well as enforce custom, acceptable use policies for thousands of employees within minutes. Appthority enables companies to leverage mobility and empower a smarter, safer, mobile workforce.

appthority
TRUST YOUR APPS

160 Spear Street | Suite 1650 | San Francisco, CA 94105 | www.appthority.com
Toll-free: 844.APP.RISK | Phone: 415.562.SAFE | | sales@appthority.com