appthority

Appthority Enterprise Mobile Security Pulse Report

Q3 2017

The Appthority Enterprise Mobile Security Pulse Report is based on millions of mobile security scans Appthority performs each quarter for its enterprise customers. The report includes app, device and network data as well as our proprietary Mobile Threat Risk Score which measures the highest risk from thousands of data points during our deep app analysis.

Appthority previously reported on data leakage risks in the Uber app. Get the report, Uber: Security Risks Come Along with Your Ride for more information.

EACH QUARTER WE PROVIDE A SNAPSHOT OF SECURITY IN THE MOBILE ENTERPRISE WHICH INCLUDES THE:

1 **TOP 100 APPS**

IOS AND ANDROID APPS IN ENTERPRISE ENVIRONMENTS, sorted by prevalence and showing the category and Appthority Mobile Risk Score

2 **TOP 10 BLACK-LISTED APPS**

IOS AND ANDROID APPS BLACKLISTED BY ENTERPRISES

3 **TOP MOBILE DATA DESTINATIONS**

BY COUNTRY FOR ENTERPRISE MOBILE DATA

TOP 100 APPS IN THE ENTERPRISE

The mobile ecosystem in an enterprise comprises apps from managed devices, BYOD and COPE. Appthority compiled a list of the top 100 apps (50 iOS and 50 Android) based on millions of scans of devices and apps in the enterprise. Using our Mobile Threat Protection solution, we determined the most common apps and their Mobile Threat Risk Scores.

Mobile threats are scored on a scale from 0-10 with zero representing low or no risk and 10 representing the highest risk level. See the Risk Scoring table at the end of this document for more information.

Among the most common apps in enterprises, data leakage risks predominate with some vulnerability risk as well.

As of August 2017:

- **The most common apps in enterprises were:**

  Android:
  Uber, The Yellow Pages, Facebook

  iOS:
  WhatsApp, Facebook Messenger, Uber

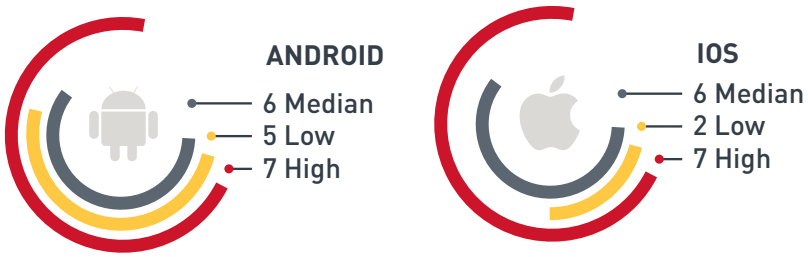
- **The riskiest apps based on the Appthority Mobile Threat Risk Score were:**

  Android:
  Uber, WhatsApp Messenger, Facebook Messenger

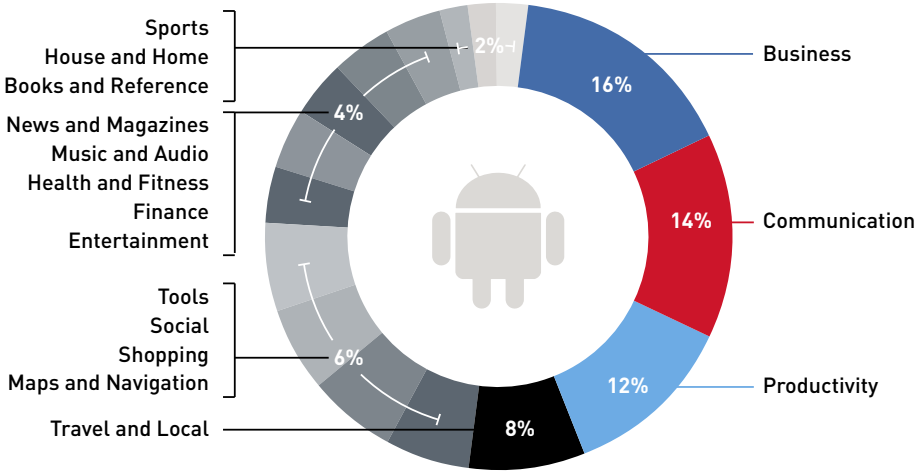
  iOS:
  Facebook, Pandora, Yelp

- Business apps are the most common category of apps in enterprises on both Android and iOS devices.

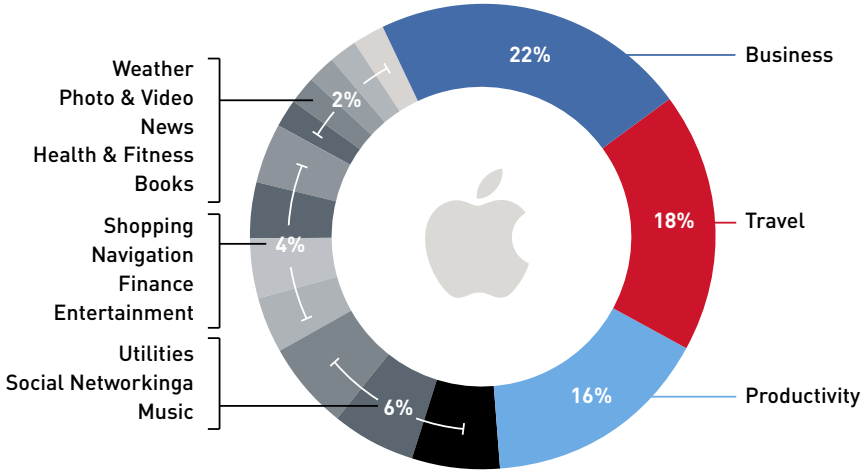
MOBILE THREAT RISK SCORES BY OS



TOP ANDROID APP CATEGORIES IN ENTERPRISE ENVIRONMENTS



TOP IOS APP CATEGORIES IN ENTERPRISE ENVIRONMENTS



TOP 50 ANDROID APPS IN THE ENTERPRISE

Rank	Application Name	Version	Category	Risk Score
1	Uber	4.160.4	Maps and Navigation	7
2	YP - The Real Yellow Pages	6.0.0	Travel and Local	6
3	Facebook	139.0.0.22.93	Social	6
4	OneNote	16.0.7967.1766	Productivity	6
5	Skype for Business	6.11.0.0	Business	6
6	Microsoft Excel	16.0.8229.2048	Productivity	6
7	Microsoft Word	16.0.8201.1009	Productivity	6
8	Instagram	10.19.1	Social	5
9	Microsoft PowerPoint	16.0.8229.2048	Productivity	6
10	RSA SecurID	2.2.1	Communication	6
11	WhatsApp Messenger	2.17.296	Communication	7
12	Amazon Kindle	4.4.0.71	Books and Reference	5
13	Facebook Messenger	132.0.0.22.90	Communication	7
14	Plenti	3.0.2	Shopping	6
15	Adobe Acrobat Reader	17.3.1.176958	Productivity	6
16	HP Print Service Plugin	3.4-2.3.0-14-17.2.17-161	Productivity	5
17	Twitter	7.8.0	News and Magazines	6
18	Dropbox	60.2.4	Productivity	5
19	VZ Navigator	10.7.6.164	Travel and Local	6
20	Keeper® Password & Data Vault	2014.01.24	Productivity	6
21	Slacker Radio	7.12.2	Music and Audio	6
22	NFL Mobile	14.2.2	Sports	7
23	Flipboard	4.0.9	News and Magazines	6
24	Peel Smart TV Remote	9.9.2.3	House and Home	6
25	Amazon Shopping	6.7.0.100	Shopping	7
26	Deutsche Telekom OnlineManager	5.2.12.118	Tools	7
27	LinkedIn	4.1.84	Social	6
28	AnyConnect	4.0.09039	Business	5
29	ANT Radio Service	41400	Communication	5
30	ANT+ Plugins Service	3.6.0	Health and Fitness	5
31	OMD Mobile	2.0.5	Business	7
32	Audible for Android	1.7.0	Books and Reference	6
33	Salesforce1	13	Business	6
34	Speedtest.net	3.2.34	Tools	6
35	IMDb Movies & TV	7.1.1.107110100	Entertainment	6
36	Spotify Music	7.4.0.1799	Music and Audio	5
37	Amazon Music	4.1.1	Music and Audio	6
38	Cisco WebEx Meetings	9.14.0	Business	6
39	Microsoft OneDrive	4.12	Productivity	6
40	Fullscreen	1.6.4	Entertainment	6
41	PingID	1.6.4(9812)	Productivity	6
42	PayPal	6.14.1	Finance	6
43	LG Health	5.31.60	Health and Fitness	7
44	Salesforce Authenticator	2.10.0	Business	6
45	Pandora Music	8.6	Music and Audio	6
46	Firefox Browser	55.0.2	Communication	6
47	Microsoft Outlook	2.2.8	Productivity	6
48	Skype	8.1.0.46539	Communication	6
49	Better Open With	1.4.10	Productivity	5
50	Snapchat	10.16.0.0	Social	6

Risk Score Legend

HIGH | MEDIUM | LOW | NA

TOP 50 IOS APPS IN THE ENTERPRISE

Rank	Application Name	Version	Category	Risk Score
1	WhatsApp Messenger	2.17.51	Social Networking	6
2	Facebook Messenger	131	Social Networking	7
3	Uber	3.258.2	Travel	6
4	RSA SecurID	2.3.0	Business	5
5	Adobe Acrobat Reader	17.07.27	Business	6
6	Pandora - Music & Radio	1708.1	Music	7
7	Spotify Music	8.4.16	Music	6
8	F5 Access for iOS	2.1.1	Business	2
9	Netflix	9.33.0	Entertainment	6
10	Amazon	9.16.0	Shopping	6
11	Concur	9.48.0	Business	6
12	Skype for Business	6.17.0	Business	6
13	Twitter	7.5.1	News	6
14	Microsoft Excel	2.4	Productivity	6
15	Microsoft Word	2.4	Productivity	6
16	Yelp	11.22.0	Travel	7
17	The Weather Channel	8.16	Weather	7
18	PayPal	6.1.1	Finance	7
19	Microsoft Outlook	2.39.0	Productivity	6
20	PingID	1.7.6	Productivity	6
21	Waze	iOS 4.28	Navigation	6
22	Pinterest	6.32	Social Networking	6
23	United Airlines	2.1.23	Travel	6
24	Microsoft PowerPoint	2.3	Productivity	6
25	Dropbox	60.2	Productivity	7

Rank	Application Name	Version	Category	Risk Score
26	Cisco Legacy AnyConnect	4.0.05069	Business	5
27	Kindle	5.13.1	Books	6
28	Scotiabank	17.7.0	Finance	6
29	Cisco WebEx Meetings	9.14.0	Business	7
30	Yammer	7	Business	6
31	Slack	3.26	Business	6
32	Speedtest by Ookla	3.8.5	Utilities	7
33	eBay	5.13.0	Shopping	7
34	Avenza Maps	3.2	Navigation	6
35	TripAdvisor	22.4.1	Travel	7
36	Fly Delta	4.4.1	Travel	6
37	Fitbit	2.39	Health & Fitness	6
38	Shazam	11.2.0	Music	7
39	Microsoft OneNote	16.4	Productivity	6
40	The Calculator	4.8.8	Utilities	7
41	Microsoft OneDrive	9.1	Productivity	6
42	Southwest Airlines	4.8.2	Travel	6
43	Genius Scan	4.1.7	Business	6
44	Airbnb	17.34	Travel	6
45	Instagram	11	Photo & Video	6
46	Amazon Prime Video	4.6	Entertainment	6
47	Marriott International	6.6.1	Travel	6
48	Hilton Honors	3.3.5	Travel	6
49	QR Reader	5.9.2	Utilities	7
50	Adobe Connect	2.6.4	Business	6

Risk Score Legend

HIGH | MEDIUM | LOW | NA

TOP APPS BLACKLISTED BY ENTERPRISES

Enterprises blacklist apps for a variety of security concerns including specific malicious or data leakage behaviors, security policy compliance, and concerns about shadow data storage.

This quarter, the top apps blacklisted by enterprises were:

Android:
Poot-debug(W100).apk, an AndroidSystemTheme, and Where's My Droid Pro

iOS:
WhatsApp Messenger, Pokémon GO and WinZip

The majority of Android apps that were blacklisted scored in the malicious range because malware was detected. iOS apps that were blacklisted scored in the data leakage range for sending SMS messages, tracking location or for sending data — including sensitive data — unencrypted.

The top app categories blacklisted were:

Android:
Tools

iOS:
Social Networking

TOP 10 BLACKLISTED ANDROID APPS

Rank	Application Name	Category	Risk Score	Score Driver
1	Poot-debug(W100).apk	Tools	9	Malware Detected
2	AndroidSystemTheme	Personalization	9	Malware Detected
3	Where's My Droid Pro	Tools	9	Malware Detected
4	Weather	Weather	9	Malware Detected
5	Wild Crocodile Simulator	Game-Simulation	9	Malware Detected
6	Star War	Not Avail.	9	Malware Detected
7	ggzzversion	Not Avail.	9	Malware Detected
8	Boyfriend Tracker	Not Avail.	6	Sends IMEI, Sends Data Unencrypted
9	Chicken Puzzle	Game-Puzzle	6	Tracks Location
10	Device Alive	Business	9	Malware Detected

Data Note: Sorted by # of orgs, then number of devices

TOP 10 BLACKLISTED IOS APPS

Rank	Application Name	Category	Risk Score	Score Driver
1	WhatsApp Messenger	Social Networking	7	Sends Address Book
2	Pokémon GO	Games	6	Accesses Address Book/Camera, Tracks Location
3	WinZip	Utilities	7	Sends SMS Messages
4	CamScanner	Productivity	7	Sends Sensitive Data Unencrypted
5	Plex	Entertainment	6	Accesses Camera, Tracks Location, Sends Device Name, Sends Data Unencrypted
6	WeChat	Social Networking	7	Sends Sensitive Data Unencrypted
7	Facebook Messenger	Social Networking	7	Sends SMS Messages
8	eBay Kleinanzeigen	Shopping	7	Sends SMS Messages
9	网易新闻 – 头条视频资讯阅读平台 (Netease news)	News	7	Sends SMS Messages, Sends Sensitive Data Unencrypted
10	Device Alive	Productivity	6	Accesses Camera Microphone/Address Book, Tracks Location, Sends Device Name

Data Note: Sorted by # of orgs, then number of devices

Risk Score Legend

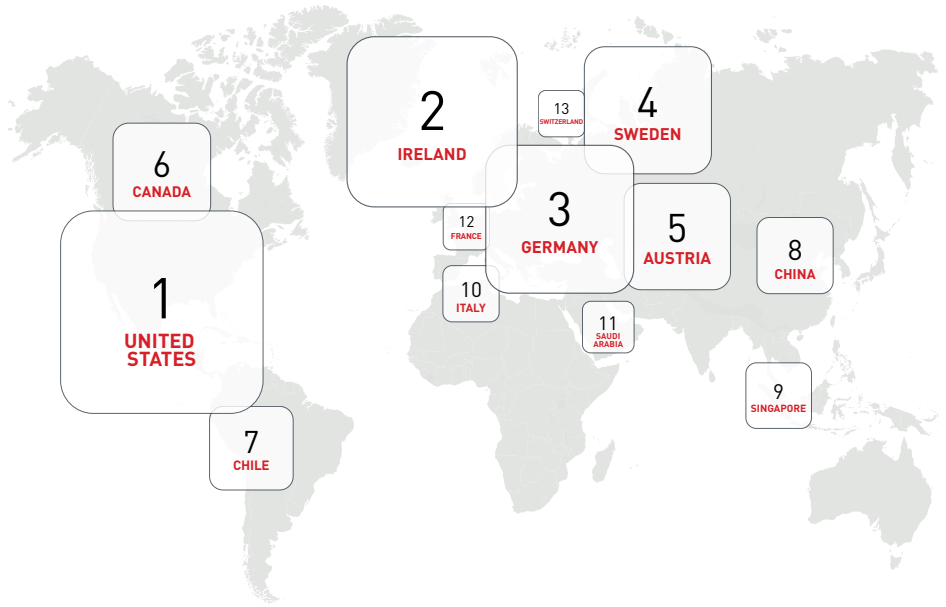
HIGH | MEDIUM | LOW | NA

TOP ENTERPRISE MOBILE DATA DESTINATIONS

A top enterprise security concern is often the countries to which mobile data is being sent. These maps reveal the top locations to which backend servers are connecting via the top 150 mobile apps in enterprise environments.

In this quarter's data, we see a difference in the profile of backend connections between Android and iOS. Android developers are connecting to a wider set of geographic locations, possibly leveraging lower cost structures overseas. Popular iOS apps have a much lower percentage of connections to countries such as China, Saudi Arabia and Chile than Android apps.

TOP 10 DATA DESTINATIONS FOR ANDROID APPS



Country	% of Connections	Site Risk				
		High	Suspicious	Moderate	Low	Trustworthy
United States	86.7%	0%	4%	34%	29%	32%
Ireland	7.7%	0%	4%	34%	22%	40%
Germany	2.1%	0%	0%	71%	0%	29%
Sweden	0.7%	0%	0%	0%	0%	100%
Austria	0.6%	0%	0%	0%	0%	100%
Canada	0.5%	0%	0%	0%	100%	0%
Chile	0.5%	0%	0%	100%	0%	0%

Country	% of Connections	Site Risk				
		High	Suspicious	Moderate	Low	Trustworthy
China	0.4%	0%	0%	0%	100%	0%
Singapore	0.3%	0%	0%	33%	0%	67%
Italy	0.2%	0%	0%	100%	0%	0%
Saudi Arabia	0.2%	0%	0%	0%	100%	0%
France	0.1%	0%	0%	0%	100%	0%
Switzerland	0.1%	0%	0%	0%	0%	100%

Risk Score Legend

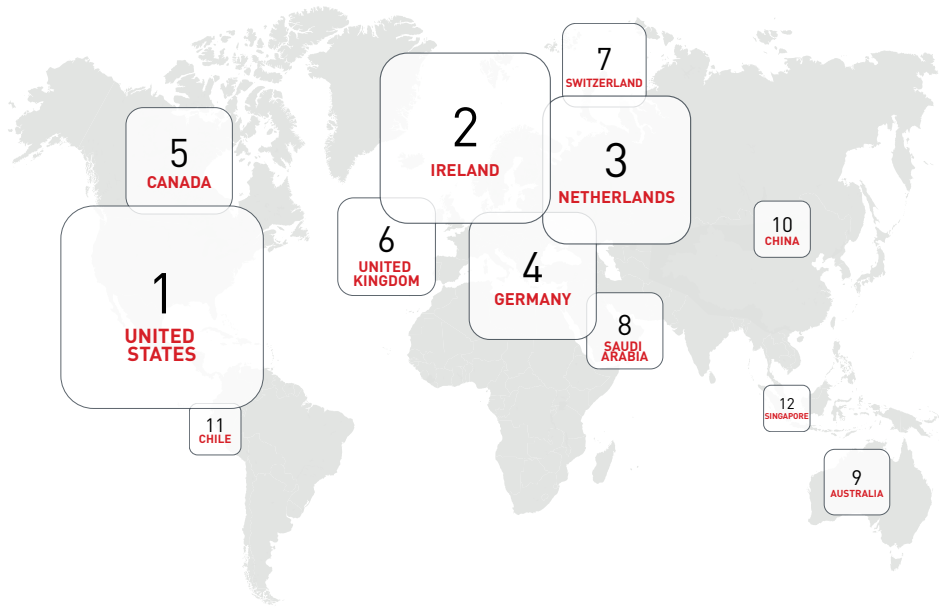
HIGH | MEDIUM | LOW | NA

TOP ENTERPRISE MOBILE DATA DESTINATIONS

A top enterprise security concern is often the countries to which mobile data is being sent. These maps reveal the top locations to which backend servers are connecting via the top 150 mobile apps in enterprise environments.

In this quarter's data, we see a difference in the profile of backend connections between Android and iOS. Android developers are connecting to a wider set of geographic locations, possibly leveraging lower cost structures overseas. Popular iOS apps have a much lower percentage of connections to countries such as China, Saudi Arabia and Chile than Android apps.

TOP 10 DATA DESTINATIONS FOR IOS APPS



Country	% of Connections	Site Risk				
		High	Suspicious	Moderate	Low	Trustworthy
United States	93.68%	0%	5%	58%	22%	15%
Ireland	3.82%	0%	6%	63%	12%	19%
Netherlands	0.86%	0%	0%	100%	0%	0%
Germany	0.86%	0%	0%	93%	0%	7%
Canada	0.32%	0%	0%	91%	9%	0%
United Kingdom	0.14%	0%	0%	0%	100%	0%

Country	% of Connections	Site Risk				
		High	Suspicious	Moderate	Low	Trustworthy
Switzerland	0.09%	0%	0%	0%	33%	67%
Saudi Arabia	0.06%	0%	0%	0%	50%	50%
Australia	0.06%	0%	0%	0%	100%	0%
China	0.06%	0%	50%	50%	0%	0%
Chile	0.03%	0%	0%	100%	0%	0%
Singapore	0.03%	0%	0%	0%	100%	0%

Risk Score Legend

HIGH | MEDIUM | LOW | NA

MOBILE RISK SCORING DETAIL

Appthority follows CVSS (Common Vulnerability Scoring System) standards in categorizing threats by broader risk types. Our proprietary scoring relies on our patented deep app analysis.

Risk Level	Category	Description
HIGH		
Score: 8-10	Malicious	A distinctly risky profile affecting mobile devices, company networks or other systems. May include malware, severe data leakage, facilitate fraud or send/steal PII and device information.
MEDIUM		
Score 6-7	Data Leakage	Accesses and/or sends enterprise related information or identifiable information — including PII.
Score 4-5	Vulnerability	Includes vulnerabilities for remote exploits or not following best practices.
LOW		
Score 1-3	Suspicious	Suspicious (but not malicious) — may indicate adware or device configuration changes.
NA		
Score: 0	Informational	Informational in nature. Identifies application behaviors useful in managing compliance with organization-defined risk policies around mobile device use (e.g., related to concerns around apps that can perform telephony actions).

ABOUT THE APPTHORITY MOBILE THREAT TEAM (MTT)

The Appthority Mobile Threat Team (MTT) monitors and investigates mobile risks that pose a direct threat to mobile enterprises. Its goal is to provide research that educates and informs enterprises looking to protect their people, data, devices, apps, and networks from mobile risks.

The MTT is comprised of top mobile security researchers and threat analytics managers who use their experience and expertise to develop best-in-class research insights. The team prides itself on delivering unique, accurate and practical perspectives, as well as security solutions, that help our enterprise audience understand and address the most impactful mobile threats.

ABOUT APPTHORITY

Appthority is a pioneer in enterprise mobile security and a leader in the Mobile Threat Defense category. The comprehensive Appthority Mobile Threat Protection (MTP) solution helps customers keep their data private and secure from mobile device, app and network threats. More Fortune 1000 companies trust Appthority to secure their enterprises from mobile threats because Appthority delivers best-in-class mobile threat protection and unparalleled enterprise visibility and control of mobile risks. With Appthority, security teams are informed, employees are productive and enterprise data is kept private and secure.

APPTHORITY, INC.
535 Mission St., 20th Floor
San Francisco | CA | 94105

FOLLOW US

CONTACT US
contact@appthority.com
+1 844-277-7475

www.appthority.com