MOBILE DATA REPORT:
JUNE 2017

Summer breaking records in temperatures, roaming data and mobile malware.

An in depth analysis of mobile data security and usage trends across Wandera's global network of enterprise mobile devices.

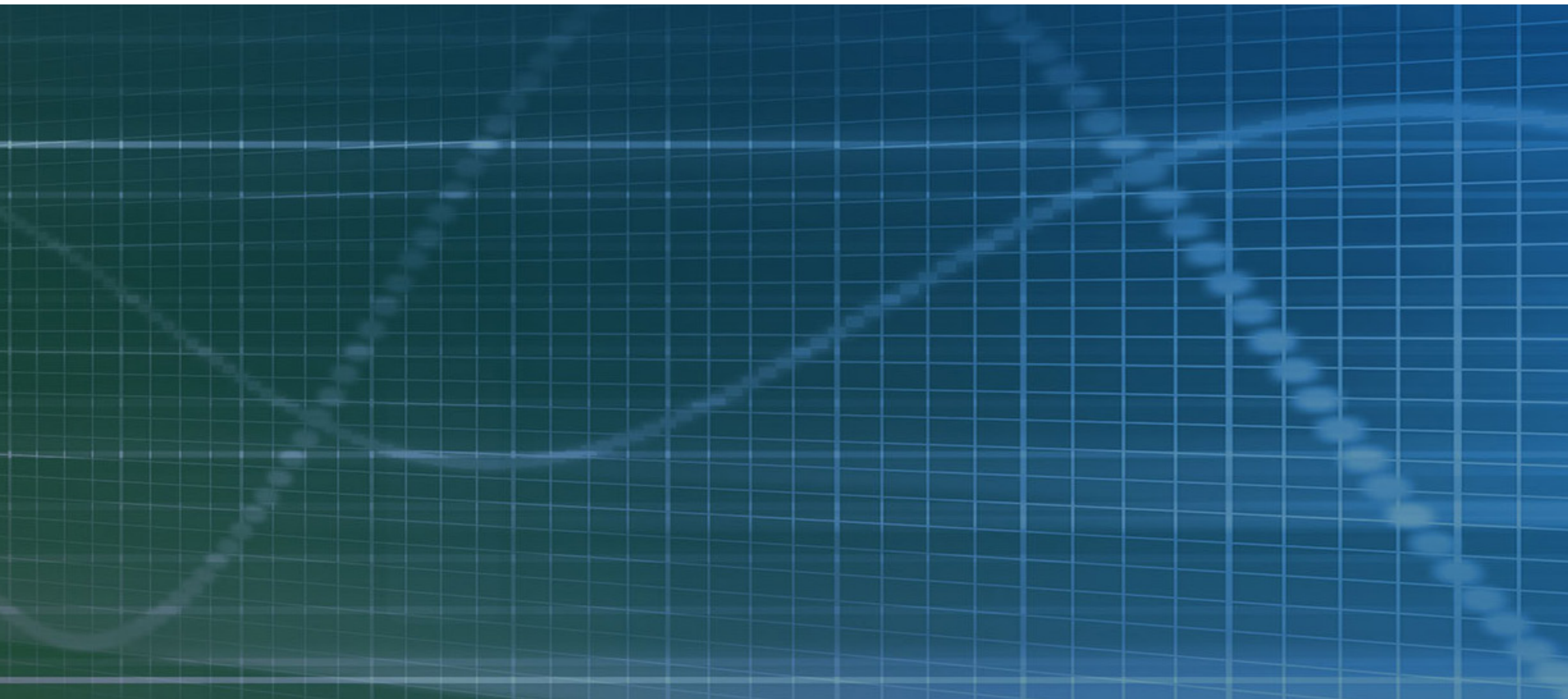
Executive summary: key insights

- The most common data leaks in June were location followed by email, username and password exposures.
- The most significant leaking app identified by the Wandera threat research team was PanicGuard, a personal safety app.
- Outdated operating systems (OS) present vulnerabilities within corporate mobile fleets. 37% of employees are using an outdated Apple OS while 80% of users haven't updated to the latest Android OS.
- Windows 10 Mobile devices were the largest driver of mobile data usage. On average they went through 82 MB of data per day, significantly more than any other type of device.
- 40% of June's total corporate mobile data was consumed by video, photo and social media apps and websites.
- Over the month, the video & photo usage category made up 22% of local data used but only 9% of roaming data.

Introduction

Our Mobile Data Report is the world's first report purely focused on enterprise mobility data. It provides a complete analysis of mobile data security and usage trends along with traffic patterns across our global network of enterprise mobile devices. These are corporate liable devices (mostly corporate owned and BYOD) used domestically and whilst roaming.

June's report is broken out into two sections. Part 1: Security and part 2: Usage. In Security, we look at the top five mobile malware culprits this month, the different types of data leaks we've detected as well as the threat of outdated operating systems on corporate mobile fleets. In Usage, we evaluate mobile usage by device type and content category. We also analyze employees' domestic vs. roaming data habits.



PART 1

Security

THE TOP FIVE MOBILE MALWARE THREATS THIS MONTH

1

XA
XAVIER
TROJAN MALWARE

XAVIER

- Xavier is an Android trojan malware that steals and leaks user information.
- It has been detected in over 800 infected applications that have been downloaded millions of times from the Google Play Store.
- The greatest number of infected app downloads originated in Southeast Asia.
- This malware uses string and internet data encryption to avoid detection.

2

JU
Judy
AUTO-CLICKING MALWARE

JUDY

- Judy is an auto-clicking malware that uses infected devices to produce fraudulent clicks on ads, generating cash for hackers.
- Between 4.5 and 18.5 million infected app downloads from the Google Play store have occured thus far..
- This variant has likely been around since April 2016 embedded within Android apps on the official store.

3

ZT
Ztorg
TROJAN SMS

ZTORG

- Ztorg is a trojan SMS malware variant that can send premium rate SMS messages and open ad URLs to siphon users' money.
- Two apps identified as hosting the malware have been downloaded over 20,000 times from the Google Play Store.
- To hide the malicious activities taking place, this trojan turns off the infected device's sound and deletes all incoming SMS messages.

5

DV
Dvmap
ROOTING MALWARE

DVMAP

- Dvmap is a new rooting malware and the first Android malware ever to inject malicious code into the device's system runtime library to gain root privileges.
- It has been downloaded from the Google Play Store more than 50,000 times.
- Hackers seem to be in the testing stage with this malware as the techniques they're using tend to break the device.
- Stay tuned for increasingly dangerous variants.

5

MA
MARCHER
BANKING MALWARE

MARCHER

- Marcher is a sophisticated banking malware that steals users' financial information.
- The malware commonly presents itself as Adobe Flash Player to be installed on the victim's device without raising suspicion.
- It waits in the background for an app to open from a targeted list of banking domains and overlays a fake login page to lure the victim into supplying credentials.
- This new variant is masterful at disguising itself. Less than 20% of antivirus scanners have been able to detect it.

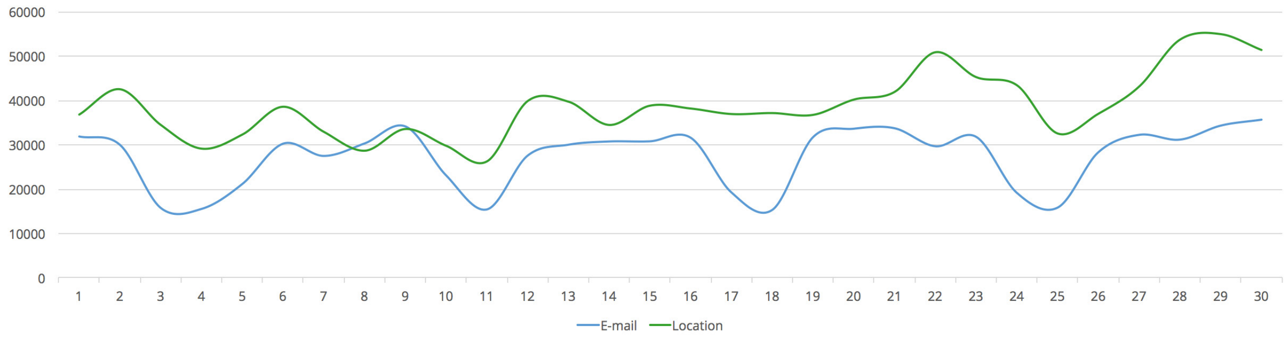
Mobile data leaks continue through June

LOCATION & EMAIL

Location leaks took the lead this month over email address leaks, demonstrating the frightening number of developers leaving users' sensitive information unprotected.

The number of sites and apps tracking users' locations has increased substantially over the last few years. Whether it's due to a steep learning curve or lack of knowledge, developers clearly haven't taken the encryption of this information very seriously.

Email leaks demonstrated a discernable pattern, exhibiting dips in volume over weekends. We believe our employed users are using their email accounts less frequently on Saturdays and Sundays, accounting for the drop in leaks. Location leaks followed a similar trend, although not as consistently.



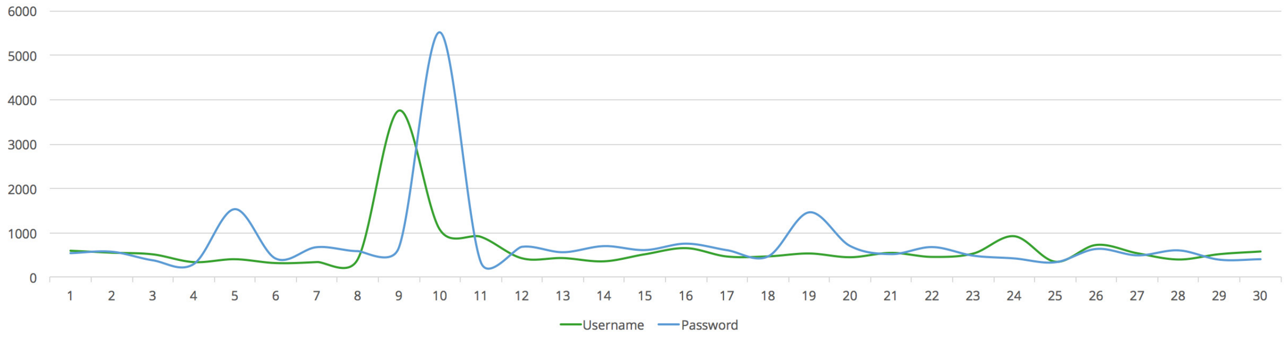
USERNAME & PASSWORD

Username and password leaks stayed relatively constant this month, with the exception of a large peak in volume at the beginning of June.

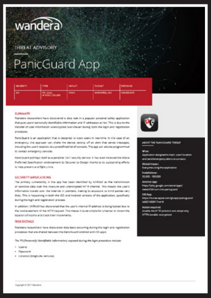
Taking a closer look at the data, this was due to two unique events occurring within our customer base. The first was the result of an employee using an online radio application that leaked his username in plaintext over 5,000 separate times in one day. The second occurred when an employee logged into the hosting website for a security camera feed. This website leaked the user's password by sending it unencrypted over the internet more than 2,000 times.

The danger inherent in username and password leaks is obvious. This information can give hackers a master key to almost all aspects of a user's life, including access to corporate email, social media and even online banking.

Preventing these leaks is as simple as developers adopting HTTPS instead of HTTP, and yet, each month we continue to see both apps and websites leaking sensitive user information.



Threat Advisories



wandera

THREAT ADVISORY

PanicGuard App

PANICGUARD

Earlier this month, we discovered a data leak in PanicGuard, a popular personal safety application that was putting users' personally identifiable information and IP addresses at risk.

The primary vulnerability in the PanicGuard app was identified as the transmission of sensitive data over the insecure and unencrypted HTTP channel.

Outdated OSs

APPLE

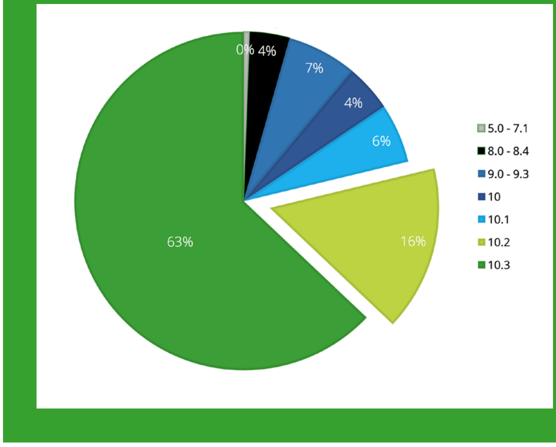
Only 63% of Apple users within our customer base have downloaded the latest iOS version (10.3). This means 37% of employees are utilizing an outdated Apple operating system.

The importance of keeping operating systems up to date is often underestimated. Exploits are increasingly discovered and published for legacy systems. Having versions as old as iOS 5 (released in 2011) within your mobile fleet presents a very significant risk.

Even recent versions of iOS have been found to have security flaws. Back in mid 2016, Apple released an OS update with an important security patch (iOS 9.3.5). This was in response to the fact that a hacker group had developed software that could read text messages, emails, calls, contacts and more through flaws in the OS.

With over 11% of users still using pre-iOS 10 operating systems, it's clear that OS security exploits should be a major concern to businesses.

APPLE iOS VERSION



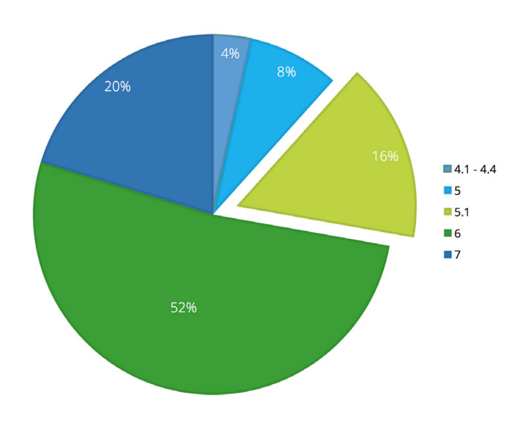
SAMSUNG ANDROID

Android OS versions present within our customers' mobile fleets appear to be even more fragmented. Only 20% of Samsung users have downloaded the latest operating system (version 7) on their devices.

This means 80% of individuals are using an outdated Android OS. Again, this is highly concerning. Any information stored on or accessed by these devices is at risk thanks to issues and bugs present within most legacy operating systems.

Android has experienced many issues with the security of its operating systems over the years and some patches have only been made available for certain OS versions. For example, a flaw identified back in 2014 that offered a way for a malicious app to hijack the trusted status of a legitimate app (by forging a digital certificate) was only fixed for Android OS versions 4.4 and later. Based on our sample of users, this means 4% of corporate devices are still exposed to this specific vulnerability.

SAMSUNG ANDROID VERSION



PART 2

Usage

AVERAGE DATA USAGE BY DEVICE

As you may already know, in March 2017 we redesigned Wandera to make it available for Windows 10 Mobile devices. We are now able to incorporate the results from these devices into our Mobile Data Report.

Windows 10 Mobile devices were the biggest driver of data usage in June. On average, Windows 10 Mobile users went through 82 MB of data per day, significantly more than any other type of mobile device within our customer base.

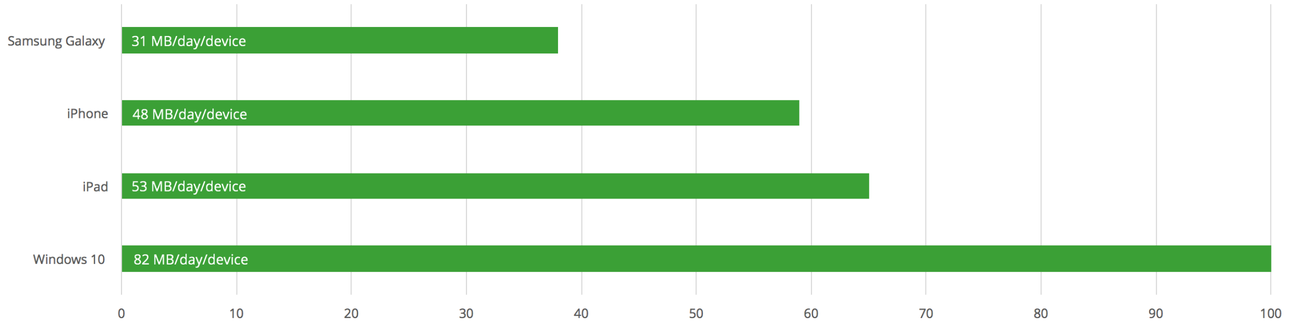
iPads came in second, hitting 65% of Windows 10 Mobile data usage. This tells us corporations are taking advantage of their company owned tablets more and more frequently. We expect this usage to continue to grow as laptops are increasingly replaced by these easily transportable devices.

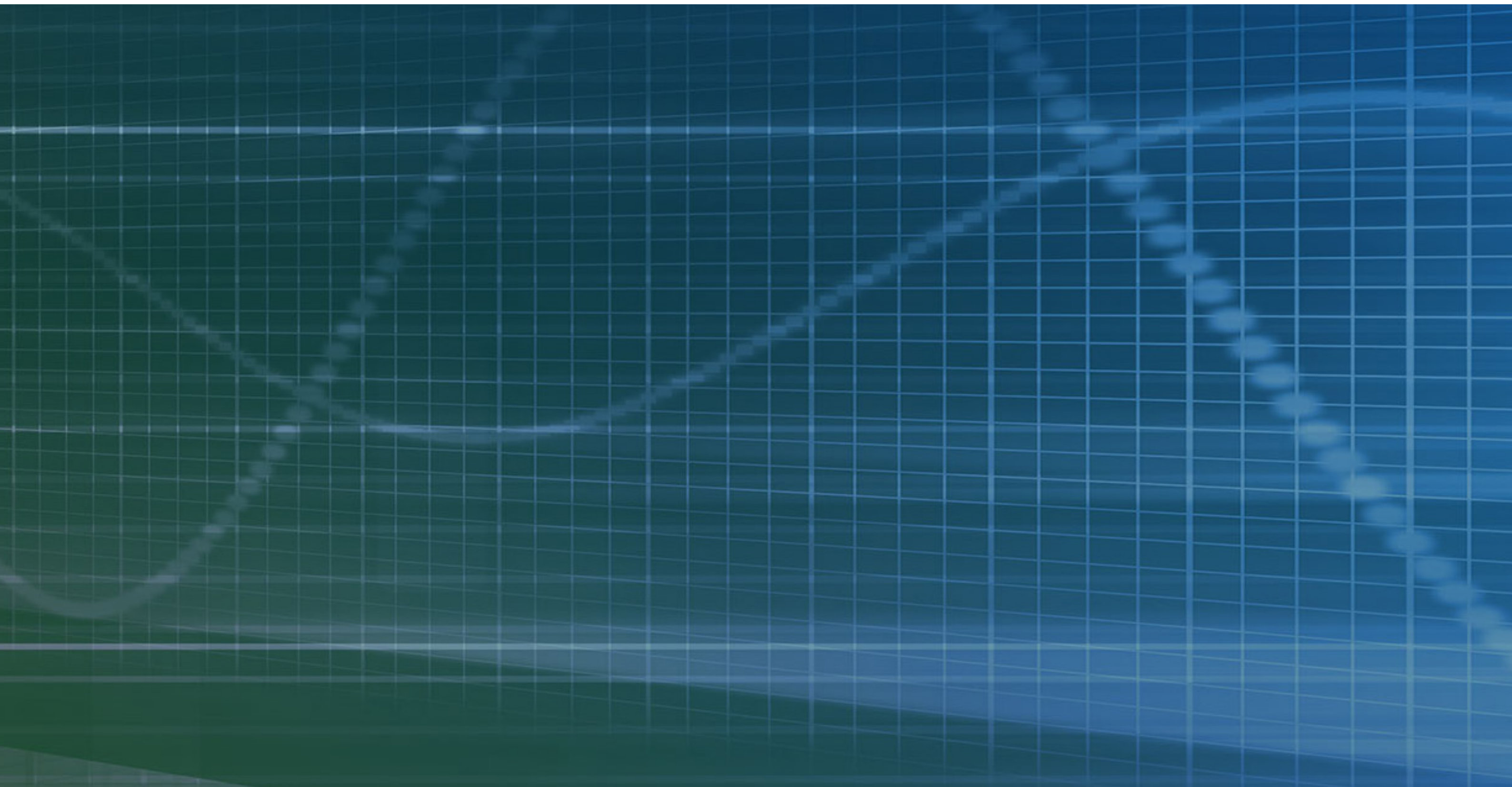
iPhones on the other hand generated only 59% of Windows 10 Mobile usage levels. This breaks the long held notion that these were the devices driving the most data usage within the corporate world.

Samsung devices used only 38% of their Windows 10 counterparts.

TOP 10 APPS BY USAGE THIS MONTH

1. Browser
2. Facebook
3. Mail
4. Instagram
5. App Store
6. SnapChat
7. Youtube
8. WhatsApp
9. Twitter
10. Spotify





THE TOP DATA USAGE CATEGORIES

It comes as no surprise that the video & photo category dominates data usage, accounting for 22% of total usage by devices on our platform. This category has the heaviest data requirements as it includes streaming video services and other data hungry applications and services.

Social media is another category that's data hungry, representing 18% of the total data used in June. Thanks to recent feature updates on Instagram and Facebook (specifically, the addition of 'Stories'), the data used by these apps and websites is at an all-time high.

Technology as a grouping hit a staggering 10% of overall data usage last month. This category includes technical service providers such as trackers, analytics and web tools such as Adobe and Google Analytics. These services aren't ones typically identified as 'data hungry' initially, but they tend to make up a significant portion of enterprise data consumption. The highest usage within the category this month came from apple.com.

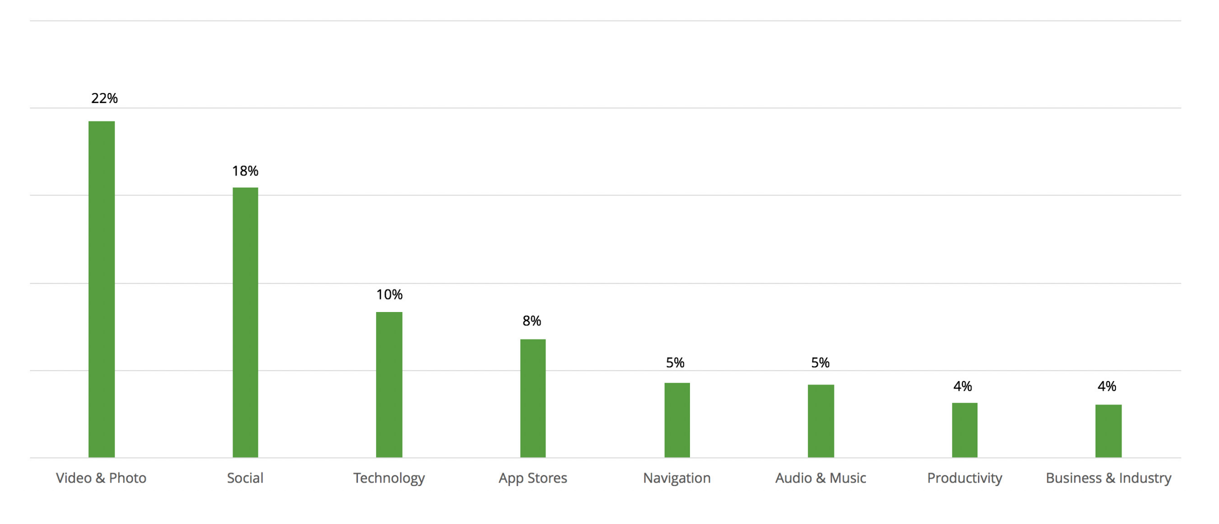
App Stores was the next largest usage category, accounting for 8% of June's data. Downloading new apps of course means utilizing data. We don't expect this user behaviour to change anytime soon and therefore, we expect this usage to remain constant in the coming months.

The next largest usage categories are music, navigation, productivity and business & industry. They all hovered at around 5% of total usage. Take a look at your own device and you might find the majority of the apps you use (outside of social media and video) fall into one of these categories. We don't anticipate any large fluctuations in these proportions in the near future.

The primary takeaway from this analysis as a whole is that 40% of data on corporate devices is spent on video & photo and social media apps and websites. This is an interesting statistic to take note of if you're responsible for maintaining productivity within your workforce.

Clearly, corporate owned devices are not being used solely for work purposes.

TOP USAGE CATEGORIES



DOMESTIC VS. ROAMING USAGE

The split

As we move into the summer months, roaming is growing as a percentage of overall data usage. June roaming came in at roughly 3%, up from 2.5% in May. We expect July and August to be the heaviest roaming months which means businesses need to ensure their potential roaming costs are managed effectively.

JUNE ROAMING

▲ 3%

TOP USAGE CATEGORIES AT HOME

1.	Video & Photo	22%
2.	Social	18%
3.	Technology	9%
4.	App Stores	8%
5.	Audio & Music	5%

TOP USAGE CATEGORIES WHEN ROAMING

1.	Social	18%
2.	Technology	13%
3.	Video & Photo	9%
4.	App Stores	7%
5.	Business & Industry	7%

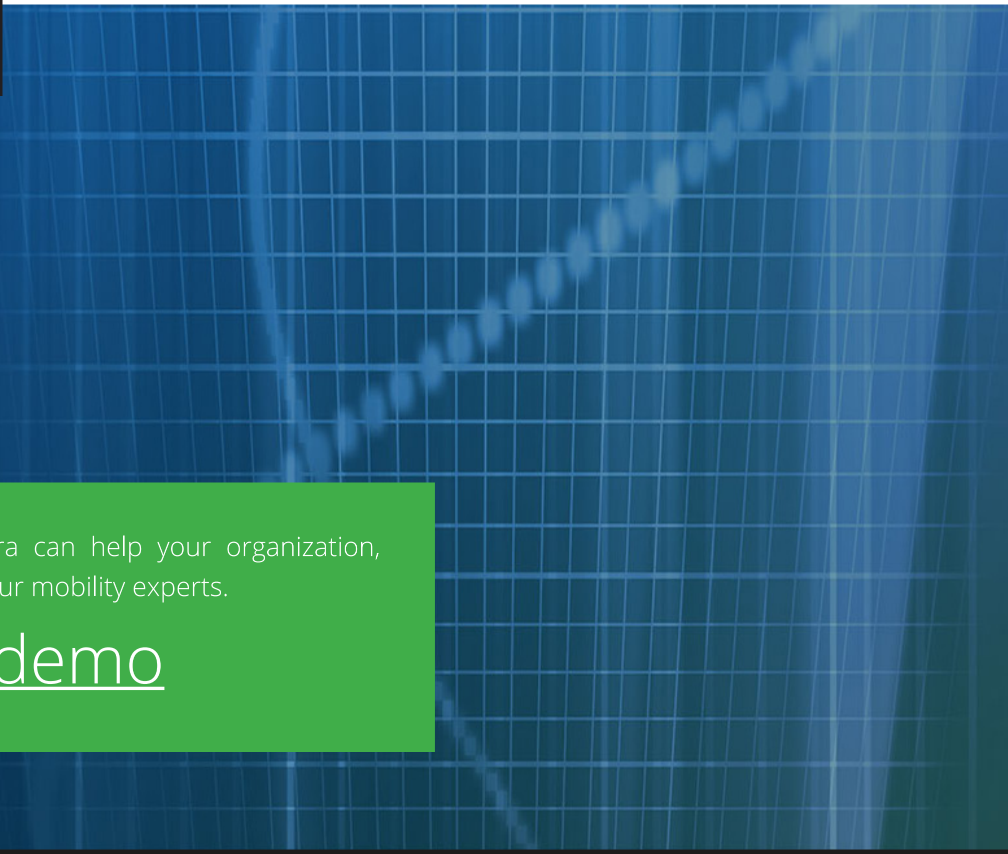
Usage: roaming vs. domestic

Individuals use their devices differently while roaming. One trend we've picked up on is that users curb their Video & Photo usage while travelling. Perhaps this is due to greater awareness of the large amounts data those apps use.

Another insight we've uncovered is that employees tend to use their phones more for businesses purposes while roaming. This leads us to believe that business trips account for a substantial portion of this roaming data. It could also however mean that those with corporate devices tend to check in regularly with the office while they are away.

Social media remains a dominant usage category regardless of whether the user is at home or abroad. Additionally, app store usage tends to remain the same whether roaming or not.

Audio & music falls out of the top five when evaluating the top roaming usage categories. We believe this may be due to users proactively downloading music to their devices prior to leaving on trips to avoid additional roaming charges.



To learn more about how Wandera can help your organization, request a demo to speak to one of our mobility experts.

wandera.com/demo

wandera

Wandera's pioneering web gateway for mobile provides organizations with Enterprise Mobile Security and Data Management.

The security solution encompasses Mobile Threat Defense and Content Filtering to prevent targeted mobile attacks, identify data leaks, and filter access to risky or unapproved usage. Wandera also offers Expense Management and Policy Enforcement, helping businesses reduce data usage, lower costs and improve productivity, delivering a measurable ROI.