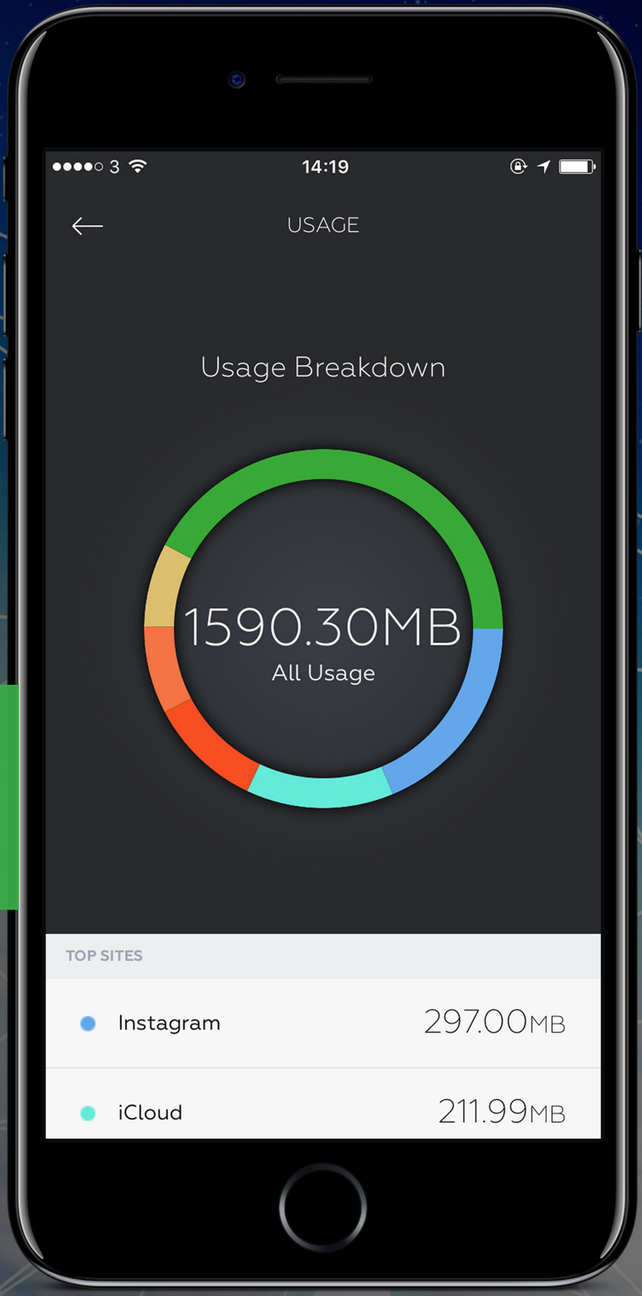
A guide to mobile cost management

This whitepaper explores the tools needed to effectively keep data costs down while maintaining productivity as well as tips for effective implementation.



TOP SITES

Instagram	297.00MB
iCloud	211.99MB

Introduction

According to research by Statcounter, it has been more than two years since mobile usage surpassed that of desktop and laptop. With the proliferation of high speed data connections and the ever increasing reliance on mobile devices, it's no surprise that data usage is increasing. While the new age of mobility can be an incredible productivity driver - allowing employees to work effectively anytime, anywhere - the costs associated with them are rising. Improperly managed handsets leave companies at risk of spiraling recurring costs and regular bill shock events.

Data visibility is the key cornerstone for understanding why costs are what they are. It is absolutely necessary for determining the right policies to put in place to prevent excessive usage whilst ensuring that mobile devices still do their job - facilitating productive employees on the go. When policies, such as capping and blocking strategies are determined, they need to be implemented and enforced, whilst still guaranteeing a pleasant end-user experience.

This whitepaper explores ways to keep on top of data costs and optimize data usage to provide value for money. It analyzes the challenges, questions and considerations involved in the implementation of a mobile data policy solution across a mobile fleet. Lastly, it looks into other benefits to an organization if an enterprise-grade data policy solution is selected.

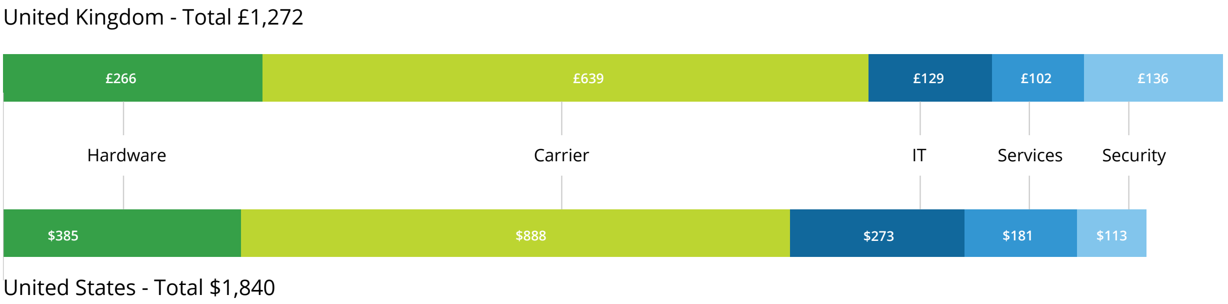
DATA VISIBILITY IS THE KEY CORNERSTONE FOR UNDERSTANDING WHY COSTS ARE WHAT THEY ARE.

Total Cost of Mobility Ownership

Enterprise mobility is an inevitable cost of doing business. Devices and connectivity are as fundamental to your operations as your employees themselves. While the decision to invest in mobility may be simple, the cost is not, particularly as mobility costs can spiral out of control quickly and unexpectedly. Remedying security breaches, roaming charges and employees' excessive data use are all ways in which mobility risks and costs can escalate.

The Total Cost of Ownership (TCO) for an enterprise is more than just the cost of the hardware and the pre-arranged monthly fee charged by the carrier. If an EMM platform is used to manage a device, its cost needs to be included. Mobility managers, security professionals and any other related IT resource should be factored in too. The costs of mobility can be broken down into fixed and variable costs: the fixed costs include hardware cost, IT spend and management platforms, which are largely inevitable; and the variable costs, such as carrier costs and security spend which, depending on company size, can be 45% - 65% of the entire cost.

Successful data cost management policies can reduce each element of the carrier costs: the recurring cost of carrier plans by 10%; the cost of necessary, variable extras (like roaming costs) by 50%; and eliminate bill shock altogether. Similarly, improved security measures such as Mobile Threat Defense solutions can remove the cost associated with security breaches, reducing the cost of security overall.



In a study run by Wandera, analysts found the actual TCO per device to be $1,840 in the US - 116% more expensive than commonly expected - which equates to $51.9 billion in total spend for American businesses. In the UK, the actual TCO per device is £1,272 - 103% more than commonly expected - which equates to £4.4 billion in total spend for UK companies

How do I control my mobile costs?

A common question people ask themselves is: "Why buy a cost management solution when I can just buy more data?" Whilst the cost of data continues to fall, it may appear that the best solution is just to invest in more data. However, does this actually help to control mobile costs?

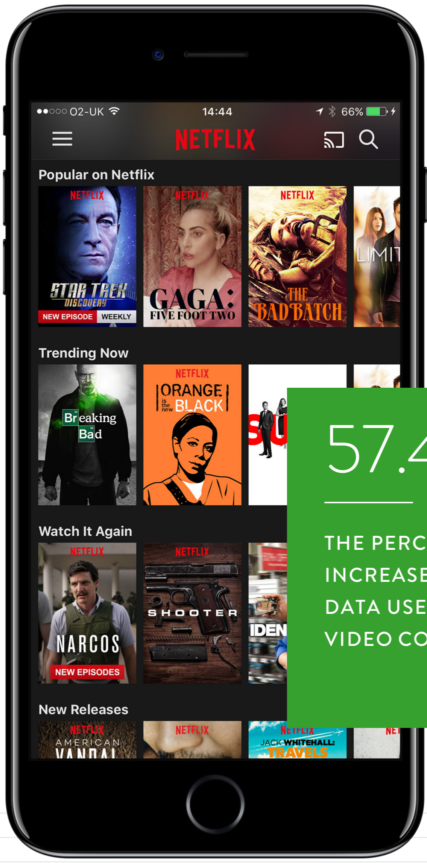
The first thought for many people looking to control spiraling mobile data costs is to go back to the carrier and either buy more data or to negotiate a new deal with a higher data allowance. Many companies use data pools or shared plans, which allow employers to have one single data allowance and share data between multiple devices. This, at best, is a short term fix. With no way to control data consumption, this can end up being an annual negotiation with charges rising steeply each year. It also does nothing to prevent employees from going over the increased data allowance.

Buying a data pool and hoping that users going over the allowance will be balanced by others who stay well beneath, is not a sustainable solution. Neither is setting a hard cap on data usage. Occasionally these solutions work, but often they won't. Keeping employees productive is a key part of mobility and a hard cap could potentially lock users out of business critical applications, negating the reason for providing the mobile device in the first place. A more sophisticated solution needs to be put into place to keep costs down while maintaining employees' productivity and connectivity.

DATA VISIBILITY

Employees are increasingly using their corporate mobile devices for personal usage. There has also been a significant rise in video streaming. Through video services, such as Netflix and YouTube, and with videos being posted on social media, there has been an increasing volume of data consumed. From our analysis, the percentage of mobile data used on video content (excluding video content viewed through social media sites such as Facebook) is up 57.4%.

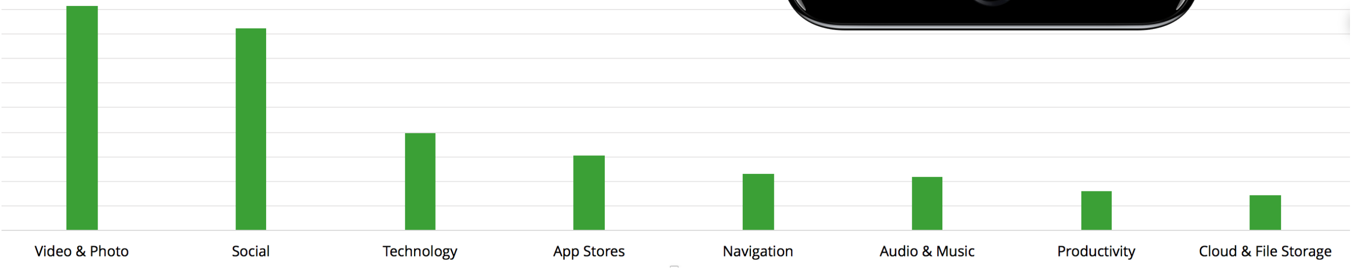
The first, and most important, part of keeping mobile costs down is understanding what you are paying for - it requires visibility of what the data is being used for. Without knowing what sites and apps employees are using, it is impossible to determine whether the cost is merited. It may be that the bulk, or even all, of the data consumed is used on business related apps and sites. Or it may be that employees are extensively using their phones for non work related activities or running up huge, unnecessary bills whilst roaming.



57.4%

THE PERCENTAGE INCREASE OF MOBILE DATA USED ON VIDEO CONTENT

WHAT SERVICES DO EMPLOYEES USE THEIR DATA PLANS ON?



EUROSTAR™

When Eurostar analyzed its own data usage, it was discovered that apps using large amounts of data in the background and staff streaming video content were major causes of excessively large bills. Rather than buy more data, the company looked for ways to optimize its existing plans. The other cause of large bills was bad user habits - people sending large files over email. This information prompted the company to take a fresh look at its file sharing policies and better educate users accordingly.

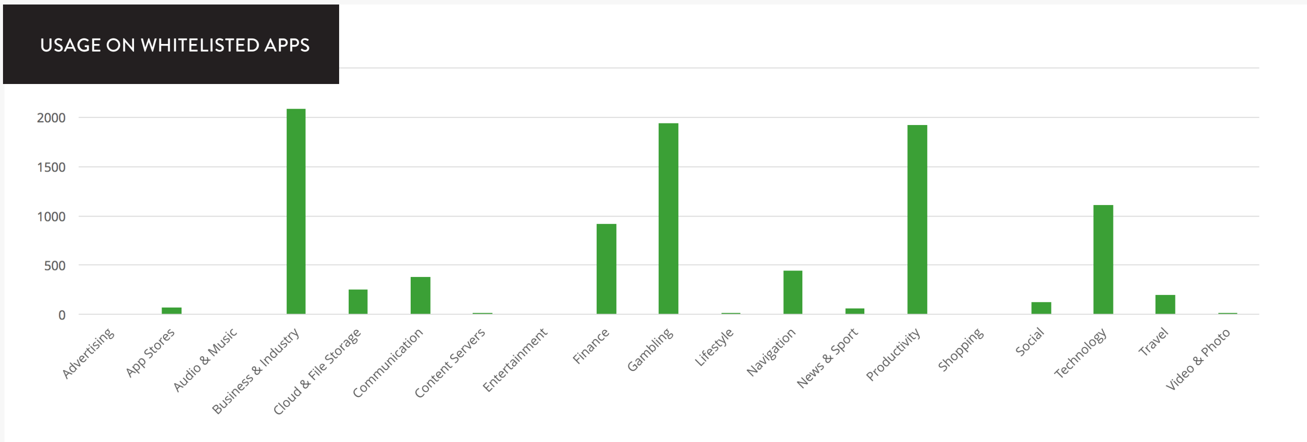
CONTROLLING ALLOWANCES

Informed capping of excessive data use is one of the easiest ways to keep costs down. On personal devices, people often set a cap if they at risk of exceeding their data allowance, limiting their use of data to Wi-Fi only and stopping themselves from getting a large bill they are personally liable for. When their employer pays for their bill, it's another matter, so the onus is on businesses themselves to be proactive with controls. However, capping data is not straightforward. Mobility is used as a business driver and as such, employees need to have the tools to be able to do their jobs, even when they have exceeded their data allowance. Simply capping data can leave employees unable to use these tools and unable do their job.

For some employees, understanding their usage and allowance is all they need to adjust their behaviour. Alerts are often effective at reducing data consumption by making employees aware of the amount of data they are using. The act of making people aware, particularly when they are getting close to their data allowance has proven successful in bringing data costs down.

Even with data insights, some users still regularly exceed their allocations. These users are ideal candidates for data caps - cutting their usage at a predetermined amount. However, any capping solution must allow business critical activities, like email, to continue. For example, a solution that offers a whitelist functionality can allow businesses to select those services that need to be accessible at all times.

> *"We had no data visibility over devices before Wandera. With Wandera you can say when, where and how...you can immediately have your questions answered.*
>
> JOHN MCGUIGAN,
> SYSTEMS ANALYST AT PERMIRA


USAGE ON WHITELISTED APPS

Data over a 3-month period in 2018. Categories using the most data are still only using about one fifth of a Gigabyte every month.

> *"One company saw savings of over 80% in some regions through notifications and awareness of a configured allowance. This is an effective demonstration of a cost management solution that supports a company culture of openness and end user responsibility."*
>
> MICHAEL COVINGTON,
> VP, PRODUCT STRATEGY AT WANDERA

OPTIMIZING USAGE

Enterprise IT has been controlling access to content on corporate computers provided to employees for decades. Extending this capability to corporate mobile devices is a natural progression, with the added benefit of helping to keep mobile data costs down. Preventing users from accessing unnecessary or undesirable material also prevents unnecessary data usage, which in turn, saves money, particularly when roaming abroad. Content filtering can also control access to expensive resources such as streaming media, downloading large files and receiving unwanted spam.

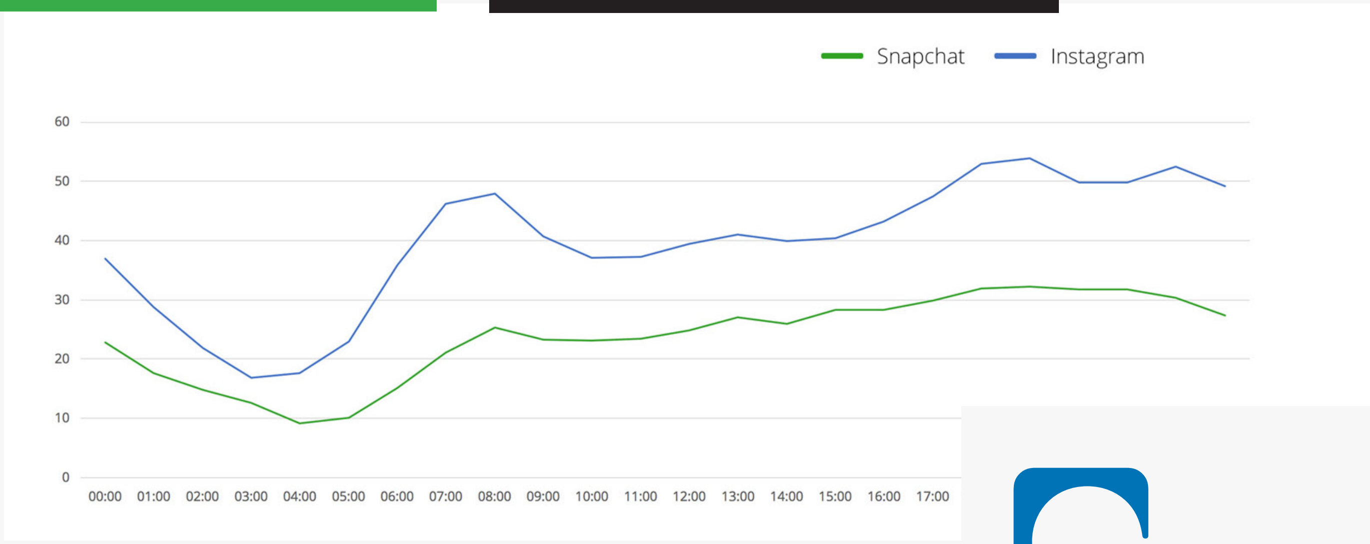
Social media use on mobile devices is also increasing. Wandera conducted research on the introduction of 'Stories' in the widely popular app Instagram. The introduction of the feature lead to an increase in usage of 146%. Increased video streaming over a cellular connection, particularly when employees are abroad, can lead to huge bill shock events.

In an increasingly global business world, it's not surprising that these scenarios become more and more common when more and more employees are passing time in airports and hotels where the Wi-Fi connection is much poorer than the readily available 4G connection. Similarly, The graph below shows the average data per device that Snapchat and Instagram use on a daily basis. With Data Management, this mass usage can be avoided.

According to recent data in our network of corporate devices, 17% of total data used was spent on social media apps like Instagram and Snapchat. This also doesn't even include video social networks like YouTube and Vimeo, which can consume significant amounts of data. That's almost $20 for every $100 phone bill.

MICHAEL COVINGTON
VP, PRODUCT STRATEGY AT WANDERA

INSTAGRAM VS SNAPCHAT USAGE THROUGHOUT THE DAY



CASE STUDY: SAVINGS

The U.S. airline Frontier found that it wasn't able to predict its mobile bills from one month to the next, due to its flight attendants regularly using their work-assigned tablets for recreational activity. This was driving up costs and making usage management extremely difficult. Creating a policy that only allowed access to work-related sites and apps, substantially reduced data consumption and eliminated all overage fees. To meet employee expectations, it allowed employees unfiltered access whenever the devices were connected to Wi-Fi. This program helped the airline save 78% on its data costs.

"People are quite happy when they receive alerts about their data usage. You can show them how non-work related usage compares to work related usage, and sometimes that's a big eye opener for people. This also deters any requests for a higher data allowance."

DYLAN JAMES, DLA PIPER

CASE STUDY: ELEVATION APP

The Elevation app features powerful content from Pastor Steven Furtick, the leader of the flock at Elevation Church. To help believers strengthen their faith, the app provides access to audio and video sermons, blog entries and other relevant information. Additionally, it allows users to actively share both podcasts and videos with friends via Twitter, Facebook and email.

For one company, Wandera found that the Elevation App used 122 gigabytes (GB) of data across two devices over a three month time period. The likely bill for the organization over those three months would be close to $2,000, driven by just two users with the app installed.

Further analysis by Wandera's data science team showed the Elevation app was repeatedly downloading the same audio and video files, causing the outlandish data usage. On one of the devices, the same 31 MB audio file of a 45 minute sermon was downloaded 6,599 times over 67 days. On one specific day, it was downloaded a total of 193 times.

It's important to realize that, in all likelihood, there was no malicious intent behind the implementation of this application. This was simply a bug that was unintentionally inflating usage. Irrespective of this, it was still costing the company money.

122GB

WANDERA FOUND THAT THE ELEVATION APP USED 122 GIGABYTES (GB) OF DATA ACROSS TWO DEVICES OVER A THREE MONTH TIME PERIOD.

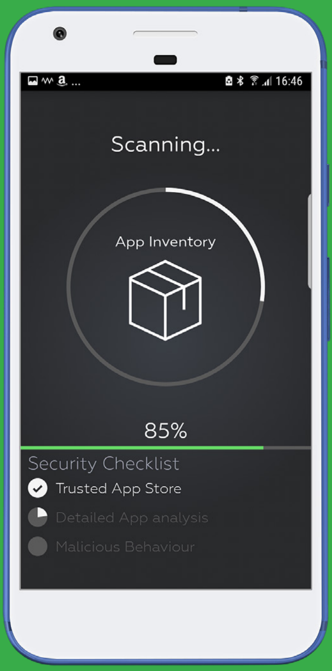
Challenges and considerations

CORRECTLY DETERMINING CONTEXT

Unsurprisingly, one of the principal driving reasons for applying Mobile Data Policy, is cost. The aim of implementing any solution is to balance the necessary cost of productivity with the unnecessary cost of overuse or wastage. To do this, there is no simple 'one rule fits all' scenario - there are many important factors to weigh up to achieve the right balance.

Who uses the device, where the device is, when the device is being used, what is the device being used for, how much the data costs - are all factors that must be considered when determining the appropriate controls to put in place. Therefore, any solution must be able to determine and support such contexts. An administrator must have a view into the data for each context in order to make informed choices when determining corresponding policy and understanding the net effect.

Equally, with mobile devices switching between cellular and Wi-Fi networks so regularly, the solution must cope with fast and regular transitions between data interfaces without imposing restrictive controls on the wrong network. Unless a Wi-Fi network is insecure or paid, it is almost universally encouraged for employees to use it if available.



THE EMPLOYEE EXPERIENCE

The user experience is an important part of any mobile solution. End users, in this case, employees, have very high expectations around their device which they are unwilling to compromise on (eg. performance, battery life). The device must also continue to perform so that it can still meet the business use case for which it was originally purchased.

Employee experience plays a large role in rising data costs. Mobile devices are likely to be in use heavily throughout the day and into the evening. However, to keep mobility productive a certain amount of personal use is to be expected. If employees are unable to use their devices in a way that closely resembles personal devices, it could make them less willing to use the device have a negative impact on productivity.

VPNs also have a significant battery impact on mobile devices and, unlike laptops, the opportunities to charge devices can be few and far between. Solutions that minimize the impact on battery life are preferred by all, particularly by end users. A mobile device that does not facilitate productivity for its owner because it is always out of battery is a less than ideal scenario, and may well outweigh the benefits of Mobile Data Policy altogether.

Such factors need to be taken into account when adopting any mobile solution. Mobile devices are with their users almost every hour of every day. A solution that inspects content flowing to and from the device, analyzes apps and protects data, all in real-time, must do so without impacting performance or the overall end user experience.

Finally, one of the most important considerations is end-user privacy, particularly on personally enabled corporate devices, and in countries with high regulations and worker councils, for example. Any mobile data policy needs to be designed to deliver on end-user privacy by securing end-user connections to increase privacy on the internet, protecting users from falling prey to phishing attacks that target user credentials and, if appropriate, completely anonymizing reports to safeguard user identities.

CHOOSING A MOBILE-FIRST SOLUTION

The complexities involved in gaining visibility of all content activity, while also maintaining a positive end-user experience, are far greater than those associated with a traditional infrastructure. On mobile devices, a mobile-first solution is essential. A solution that blends on-device and transparent cloud gateway characteristics, leveraging the unique abilities of the platforms, is a must, providing a consistent and reliable umbrella over the fast-growing and inconsistent device landscape.

Beyond cost, what else should I consider?

While the new age of mobility can be an incredible productivity driver, there is more to consider than just the cost associated with running a mobile fleet. Work assigned devices are introducing rising levels of risk to the enterprise. Improperly managed handsets leave companies at risk of security issues, productivity losses and exposed to potential litigation.

The ease with which mobile devices can access many disparate networks, both inside and outside of the office means they are becoming increasingly difficult to manage. Employees can easily access and download material which is not accessible within the corporate network including illegal and illicit content creating issues not just for IT, but fot Human Resources and the legal department.

CONTENT FILTERING

Content filtering can serve to solve many more problems than just keeping costs down - it can help with the most difficult mobile challenges.

PRODUCTIVITY

The mobile device is a distinctive technology that delivers tangible benefits in both personal and business settings. According to IDC's U.S Mobile Worker Forecast, mobile workers will account for nearly three-quarters (72.3%) of the total U.S. workforce—or 105.4 million employees—by 2020, creating an environment where workers expect to leverage mobile technology at work.

Although CSOs/CIOs and their teams are tasked with maintaining information security, they must also support and help maintain employee productivity. This includes putting mechanisms in place that stop workers from engaging in time-wasting activities. A highly portable mobile device presents a unique challenge when compared to locked down traditional infrastructure, because the user has access to web surfing at anytime they desire, as well as games and apps that disrupt their work. Wandera data suggests that most corporate devices are used for recreational activity for an average of 60 minutes during a typical working day.

SHADOW IT

Shadow IT refers to the introduction of unapproved technical services that conflict with existing IT policy or competing services. On traditional IT infrastructure, there are numerous tools and mature user expectations to help administrators control Shadow IT. However, with extensive mobile device usage being relatively new to the corporate world, a lack of effective tooling and differing end-user perception of device policy, IT departments are struggling to implement similar, effective policies across their mobile fleets.

Mobility is an especially hard platform to eliminate shadow IT on, because it is more difficult to manage a device that can connect to so many different networks. IT is often unaware of which apps are downloaded, which websites are visited, or which services are accessed. The problem becomes even more difficult when considering sites and apps that can be used for both business and personal use, and whether they are used for harmless or nefarious purposes.

LEGAL LIABILITIES

Corporate liability and vicarious liability laws ‘hold employers liable for the actions of their employees’. These laws apply to all actions within the scope of employment and often pertain to acts which cause harm to another person. Vicarious liability holds employers accountable for the wrongful, negligent or the intentionally tort actions of their employees. Courts can, and do, find employers responsible for their employees’ actions, often leading to large fines and damage to company reputation. With the electronic revolution, employers can be found liable for misuse of email, the internet and company devices, in addition to more traditional employee activities. For example, courts have found companies liable for sexual harassment when co-workers have used the internet to view sexually explicit pictures on their work laptops, copyright infringement, and more recently social media interactions.

SECURITY

The ability for mobile devices to access all corners of the internet introduces added risk into a business’ infrastructure. Each of the major app stores has over one million apps, with many more being added each day. The quick turnaround expected of app designers and the emphasis on usability means security falls to the bottom of the priority list when it comes to getting apps on the market. Even apps on official stores have been found to be lacking in key areas of security.

Enforcing an acceptable usage policy for mobile devices is a solid first step toward better security. However, to truly protect the enterprise, an appropriate mobile threat defense solution is also a must-have.

Summary

Mobile data is the black hole of the modern IT team - but it doesn't have to be.

Wandera's transparent cloud gateway for corporate-owned mobile devices provides best-in-class Mobile Data Policy functionality, allowing admins to control access to a large number of sites and apps using an intuitive dashboard.

As demonstrated in this white paper, Mobile Data Policy is essential for controlling costs and the right solution can solve further challenges across the organization. Wandera has been designed to meet these challenges, providing enterprise-grade data controls on a proactive and highly visible level. These features can also be used to enhance employee productivity and protect companies from legal liability and security risks.

To explore how this technology could benefit your organization, get in touch with one of our experts.

wandera.com/demo

wandera

Wandera is a leading mobile security company, providing multi-level protection against cyber threats for users, endpoints, and corporate applications. Security teams worldwide rely on Wandera to eliminate threats, control unwanted access, prevent data loss and enhance user privacy. The company pioneered the application of data science to tackle the complex challenges of mobile security with MI:RIAM, the industry's most effective threat intelligence. Recognized by analysts and trusted by thousands of enterprise customers, Wandera was founded in 2012 and is headquartered in San Francisco and London. To learn more visit www.wandera.com, or follow on LinkedIn and Twitter.