wandera

A Guide to Content Filtering for Mobile

The challenges, trends and benefits of Content Filtering in a mobile-first environment

TABLE OF CONTENTS

INTRODUCTION

According to research by Statcounter in 2016, mobile usage has now surpassed that of desktop and laptop. While the new age of mobility can be an incredible productivity driver - allowing employees to work effectively anytime, anywhere - work-assigned devices are also 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 and control by enterprise IT departments. Employees can easily access and download material which is not accessible within the corporate network, throwing up issues of shadow IT, data exfiltration and more.

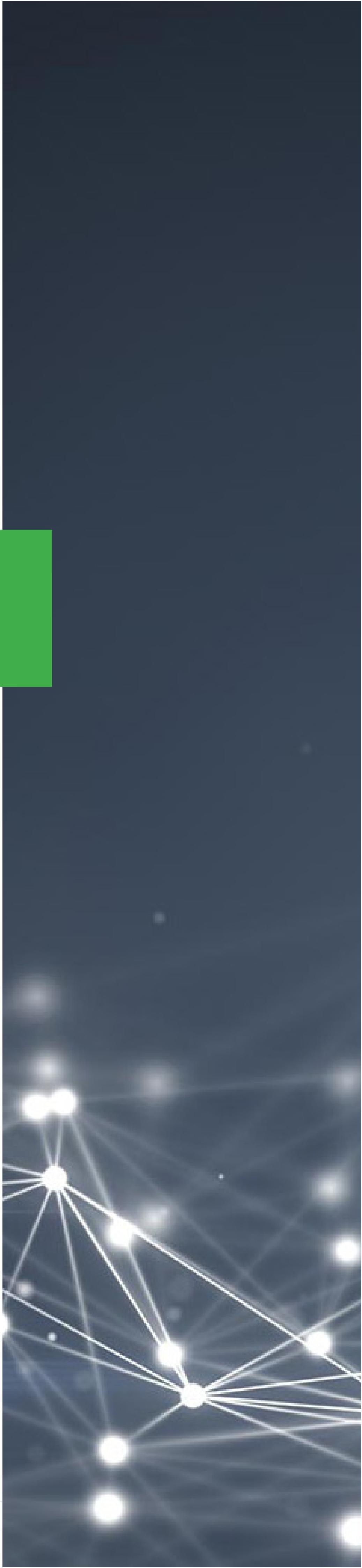
However, the issue goes beyond technology administration. The ability for employees to access illegal and illicit content on corporate devices may generate a number of issues for both the human resources and legal departments.

MOBILE USAGE HAS NOW SURPASSED THAT OF DESKTOP AND LAPTOP

Mobile devices are also inherently different to desktops and laptops. The crossover between personal and work usage is more blurred. Employees regularly use their work-assigned devices for recreational use and usually expect to be able to do so.

Content Filtering is often viewed as a draconian solution, depriving employees of this freedom. The reality is that it can not only solve many of the most difficult mobile challenges facing enterprises today, but also that it provides benefits that might have otherwise been unforeseen by IT leaders.

This whitepaper explores these benefits, analyzing five main areas: Shadow IT, security, productivity, legal considerations and expense management. It also analyzes the challenges, questions and considerations involved in the implementation of Content Filtering across a mobile fleet.



The benefits of Content Filtering

AN OVERVIEW

For decades, enterprise IT has been controlling access to content on corporate computers provided to employees. As these computers became more capable and increasingly connected to the internet, the possibility for employee misuse became significant. Companies put policies and solutions in place to reduce this risk, and to make it clear where the boundaries were.

Although initially seen as an IT problem, it eventually became an HR or management problem, having to be addressed at both corporate culture and technology levels. As similar changes happen to mobile devices, with more and more people using them for work (beyond a simple phone call), the same problem has again resurfaced.

In a mobile context, it is still important for devices to adhere to security regulations and policy, whether set by IT, HR or the legal department. When engaging in mobile-focused conversations it is important to articulate what 'Acceptable Usage' policy is and why it should be followed.

This includes specifying which operating systems are allowed, which apps are approved for download and use on the corporate network, which classifications of websites are allowed and which cloud services are supported and authorized.

THE TREND

The large majority of companies enable some form of web content filtering within the corporate network, ensuring coverage of traditional IT infrastructures. Typically this will include some level of control for the sites and services that employees can access on work-assigned computers.

In the few instances where filtering is not in place, there will almost always be systems present that provide visibility into usage.

Whilst visibility alone is not a mechanism for ensuring productivity, network efficiency or minimizing the risk of liabilities, it is considered a standard requirement for enterprise. It provides a starting point to determine whether taking any further action is necessary. For this, companies use technology such as Secure Web Gateways and Next Generation Firewalls, both of which are multi-billion dollar markets.

However, only recently have companies begun to seek the same level of visibility and control over mobile devices as they have for assets within the traditional network. This trend is largely driven by:

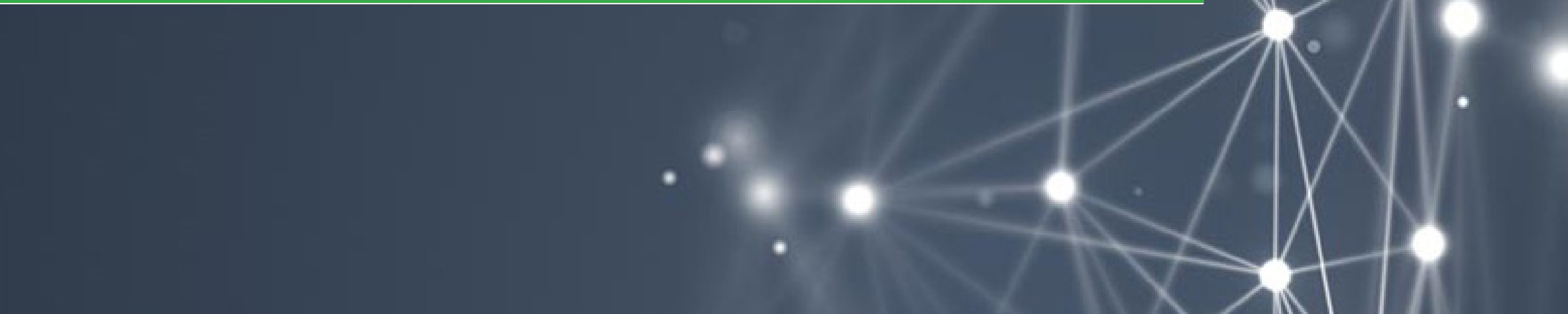
1. Mobile's increased share of overall usage – now hovering around 50% for knowledge workers. With so much work now happening on mobile, the ability to discover and control data becomes critical.

2. The significant confusion from employees as to what constitutes acceptable use on mobile. Unlike traditional PCs, there is a stronger perception that mobile devices, even when corporate owned or corporate liable, are 'unmanaged' employee devices. Despite this, the company can be held legally liable in the event of an incident.

3. A greater opportunity for information leaks or productivity drain. The long tail of over four million apps that can be easily installed by users makes potential unapproved usage much more likely. The same is true for the countless website and domains accessible via mobile web browsers.

4. The overall lack of visibility for administrators into how users are engaging with apps and content through their mobile browser. Carriers often provide only aggregate data usage with limited granularity.

5. The impact of reduced controls as organizations have transitioned from Blackberry to new consumer-centric platforms. This is only starting to be addressed, for example, in Apple's recent focus on introducing Device Supervision capabilities (as part of its Device Enrolment Program). On Supervised Devices, enterprise-level controls, similar to those offered by Blackberry, are being introduced to begin to address the imbalance and return some control from users to the enterprise.



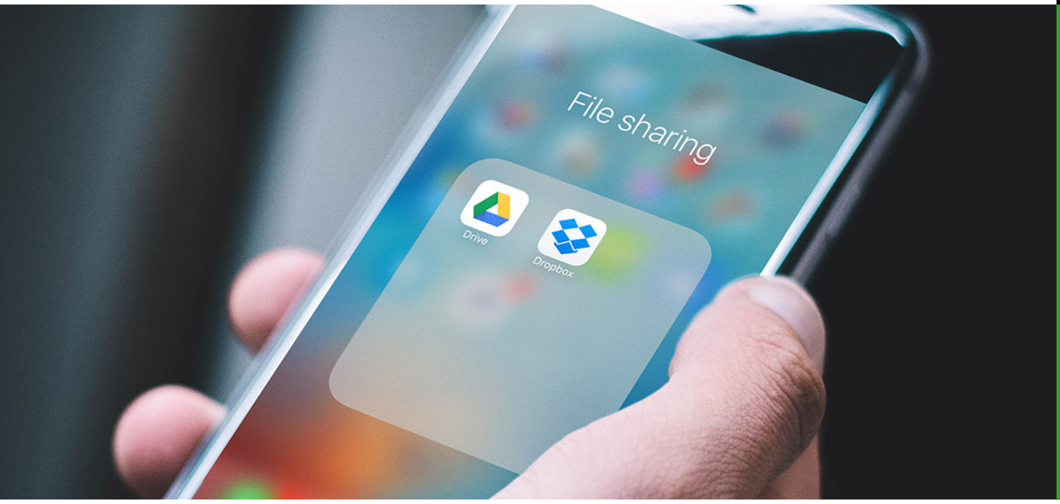
CONTENT FILTERING FOR

Shadow IT and File-Sharing

Compliance with corporate IT policy is essential for ensuring that corporate devices remain up-to-date with the right security, software and hardware. IT departments invest a lot of time on RFPs, evaluating tools to ensure they select the most fit for purpose. Significant time is spent making sure these tools are configured and set up correctly. It takes a lot of resource to get the right tools in place to facilitate efficient, secure employee work.

Shadow IT refers to the introduction of unapproved technology that conflict with existing IT policy or 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.

> *"We're finding that the mobile device is often used to circumvent some of the protections and controls the enterprise has put in place within its own infrastructure. Whether it's deliberate or accidental, use of unsolicited services is undoubtedly the most common way that sensitive data gets exposed"*
>
> MICHAEL COVINGTON
> VP OF PRODUCT AT WANDERA.



11%

THE SHARE OF RESPONDENTS ADMITTING TO USING UNAPPROVED FILE-SHARING SERVICES SUCH AS GOOGLE DRIVE, ICLOUD AND DROPBOX ON WORK DEVICES.

Mobile 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. Companies are 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 being used for harmless or nefarious purposes.

In some cases, employees are unaware that their actions are a risk to the corporation. The most prominent example is filesharing. Employees will often use external (or even personal) file-sharing services such as Dropbox or Google Drive to share business related documents. If sensitive information is being shared outside of approved tooling then a breach to the service or poor password management could mean the data ends up in the wrong hands. Worse still, the company would be none the wiser.

CASE STUDY DATA LEAKS

A well-known European retail bank found that it was continually suffering leaks of sensitive corporate data even though its internet policy had been strictly enforced. From analyzing the source of these events, it was discovered that these leaks could be traced back to employees using their mobile data connections to circumvent policy and upload classified company documents. In one case, this was a deliberate action of a disgruntled employee about to join a competitor, but in other cases, it was simply a matter of employees trying to work as efficiently as possible and not understanding the impact of their actions. Through the implementation of a mobile Content Filtering solution alongside a company-wide education program, the company managed to prevent any further data leakage incidents.

> *"In order to make an online bet or play an online game involving money, you must first create an account and deposit funds, immediately you are incurring a higher degree of risk than you would by placing a wager at your local bookmakers or card room because you are sharing sensitive details online; age, identity, email address, bank account number, sort code, all now have a digital manifestation.*
>
> *On a very simple level, if you don't have some form of security in place then these details are easily available to anyone with the technical know-how, and there are a lot of people with this sort of knowledge meaning investing in security software is pertinent."*
>
> BRIAN CODY
> NORTON SECURITY

CONTENT FILTERING FOR

Preventative 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.

On top of this, it has been found that adult sites, gambling apps and other content categories have been proven to be far more likely to leak data, employ unencrypted technologies and otherwise expose organizations to increased risk. Content Filtering provides a proactive approach to security, allowing for the ability to block the more risky sites and apps, helping to eliminate exposure to many threats before they manifest.

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

CASE STUDY: PROACTIVE BLOCKING

One large home repairs company found that it was experiencing a handful of high-risk security events every month. It noticed that many of these were originating from activity undertaken on mobile devices. Upon closer inspection, most of these could be traced to services accessed in the adult and gambling categories. After implementing Content Filtering across its mobile fleet, the volume of monthly security events was reduced by more than 30%.

80%

40 OF THE TOP 50 ADULT SITES WERE FOUND TO CONTAIN SECURITY VULNERABILITIES AND WERE EXPOSING SENSITIVE DATA TO POTENTIAL ATTACKERS

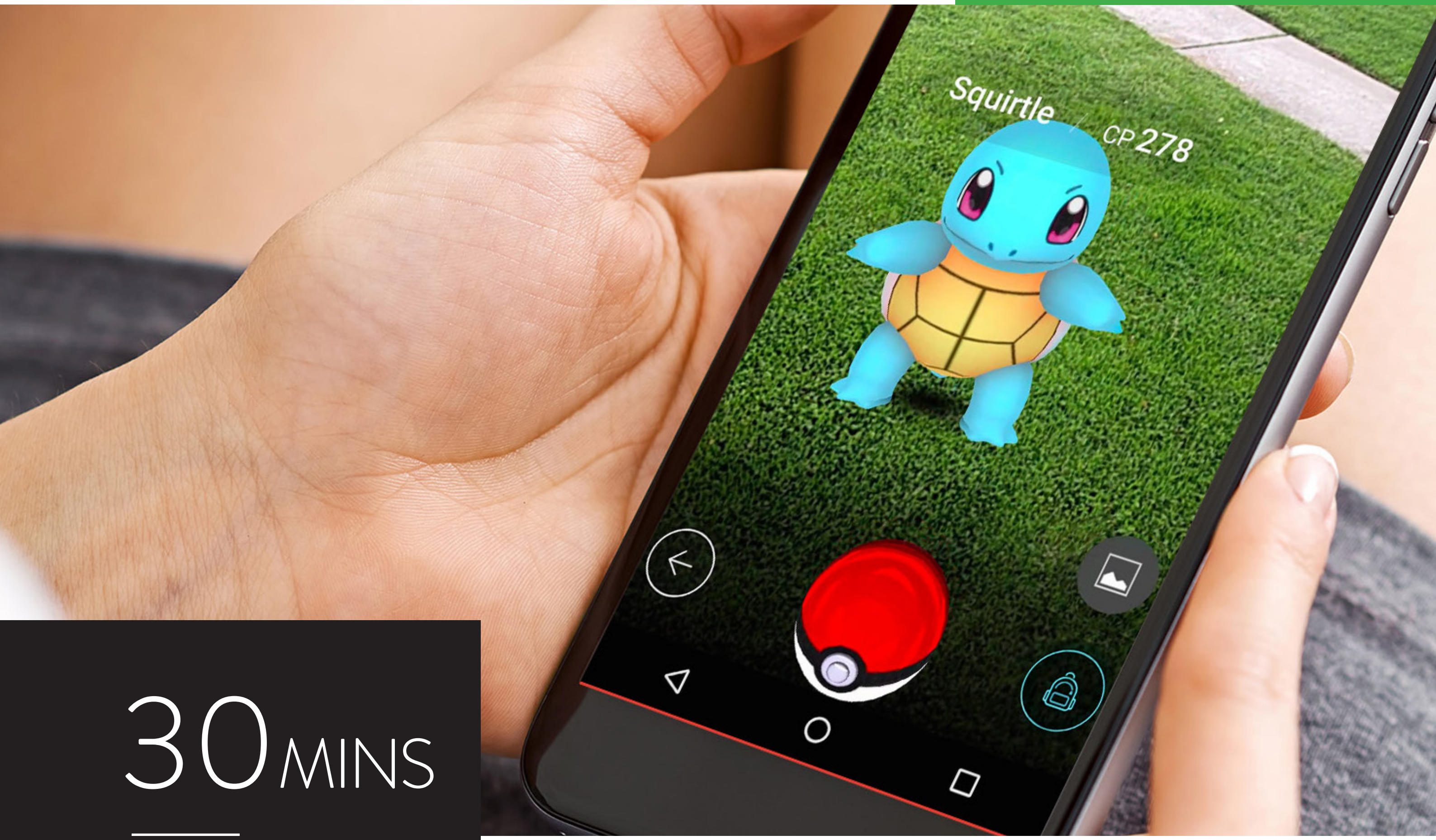
CONTENT FILTERING FOR

Productivity Gain

The mobile device is a distinctive technology that delivers tangible benefits in both personal and business contexts. 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 the CIO and their team 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 30 minutes during a typical working day.

> *"How many times have you looked around your office and seen your employees with their heads down? Everyone uses their mobiles for occasional personal use within working hours for things like Facebook or news sites. This in itself may not necessarily be an issue, but it doesn't mean you'd want to encourage the behavior. By blocking content such as games on work corporate devices, it's easy to draw where the line is. This not only keeps productivity levels from slipping but also sends a clear message to your employees about what is and what isn't acceptable."*
>
> SENIOR HR MANAGER AT A EUROPEAN RETAIL BANK



30 MINS

AVERAGE TIME SPENT ON RECREATIONAL MOBILE USE BY EMPLOYEES DURING TRADITIONAL WORKING HOURS

CASE STUDY: POKEMON GO

By July 2016, Pokemon Go had been downloaded 75 million times and was used by over 21 million daily users. Although the app itself consumed relatively low amounts of data, the concern for some companies was the amount of time their employees spent on the app, and whether they were using it during work hours. The loss of productivity became a huge concern. Having a Content Filtering solution on their mobile devices allowed customers to block Pokemon Go from corporate phones, eliminating the productivity drain.

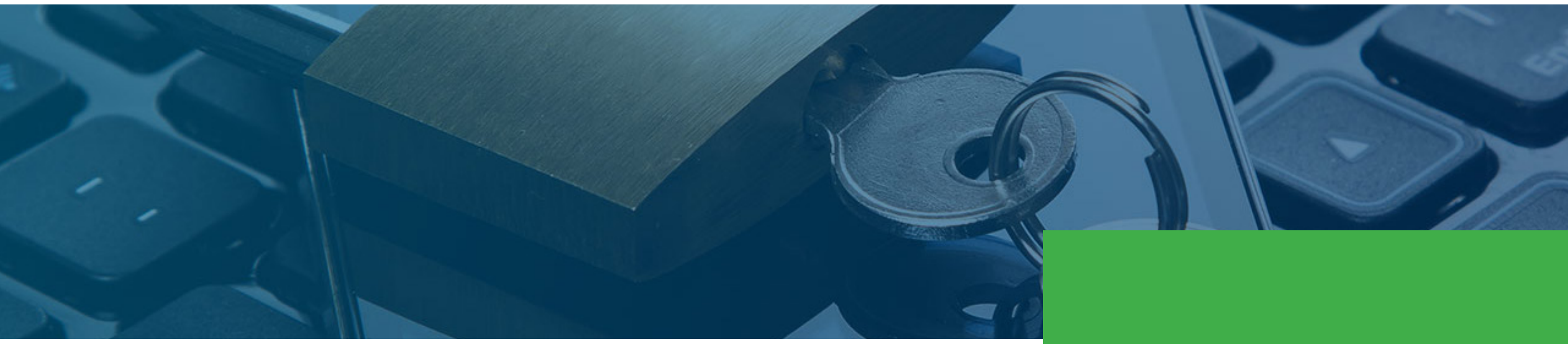
CONTENT FILTERING FOR

Legal Considerations

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. Courts have found companies liable for sexual harassment when co-workers have used the internet to view sexually explicit pictures on their work laptops.

Employers may also find themselves liable if employees infringe copyright. One lawsuit found the employer liable when its employees copied and retained copyrighted product support manuals and diagnostic software, which was then used in their contracts to perform service and maintenance for their clients. By preventing workers from using peer-to-peer networking sites to download copyrighted music and videos, employers could help avoid lawsuits. Peer-to-peer apps are increasingly appearing on mobile devices. This increase combined with the high speeds of 4G connections and the portability of devices, results in users downloading more and more content on their mobile devices. In addition, employees using their corporate owned devices for personal use may increase the recurrence of copyrighted downloads.

Although companies do not have the duty to monitor the private communications of their employees, the Human Resources department must ensure that no employee is subject to an intimidating, hostile or offensive workplace. Preventing employees from accessing content that includes pornography, weapons and hate speech can help reduce inflammatory materials in the workplace. An employer’s duty of care is now extending to interactions through social media, often primarily accessed through corporate mobile devices. An easy way to simplify this job is by restricting access to social networks on corporate devices unless they are absolutely necessary for an employee’s job role. In addition, HR may also be responsible for managing a social media policy that provides guidelines on how employees should and should not post information and express opinions on social media sites, blogs and community websites and forums.



CASE STUDY: CHILD ABUSE

One company based in the UK was liable for damages when one of its employees was viewing child pornography online at work. The court found over 1,000 pornographic images on the individual’s work device, and the employer was found to be partially responsible for the offence.

CASE STUDY: PORNOGRAPHY

Employees from the US Government were persistently accessing pornography on their work devices. Again, in this instance, the US Government was held responsible. In both case studies, each company had an internet usage policy, but there was no active monitoring or enforcement in place. Furthermore, while these policies existed for laptops, it did not extend to mobile - a huge oversight when considering the potentially expensive legal ramifications.

4%

OF ANNUAL REVENUE

THE PENALTY FOR COMPANIES FAILING TO TAKE REASONABLE MEASURES TO PROTECT PERSONAL DATA, INCLUDING MOBILE, UNDER NEW GDPR LEGISLATION

CONTENT FILTERING FOR

Mobile Expense Management

Content Filtering on mobile devices also provides an opportunity to gain a tangible return on investment. Preventing users from accessing undesirable material also prevents unnecessary data usage, which in turn, saves money, particularly if this usage was done when roaming abroad, where data costs are notoriously high. When combining this across all users and their devices, it can represent significant savings to the enterprise.

Streaming media, downloading large files and receiving unwanted spam are, for many organizations, among the top bandwidth hogs.

Content Filtering can be used to control access to these expensive resources, reducing data consumption. Even though usage may be unintentional, as almost all mobile devices have an always-on data connection, they have the potential to be misused, both deliberately and accidentally.

In fact, research shows that, for Wandera customers, there was a percentage growth in video content usage from 5.2% to 57.4% between January to May 2016 using mobile data. This steep increase can be attributed mainly to the use of personal apps such as YouTube and Netflix. Streaming video over a cellular connection, particularly when employees are abroad and passing time in hotel rooms and airports, can lead to huge bill shock events, which can be avoided using Content Filtering.

Content Filtering is not just a blunt tool for restricting access either. With real-time access to the mobile activity of staff, mobility admins can create alerts and workflows to address data consumption issues as they emerge, or customize policy depending on the department, for individual users or during expensive overseas trips.

Notifications and analytics are helpful for both admins and employees alike. Research from Wandera has shown that simply alerting users to their data usage in real time, via an app on their device, helps inspire behavioral change and provoke user-driven cost reduction.

35%

AVERAGE SAVINGS ON DATA COSTS AFTER CONTENT FILTERING IS IMPLEMENTED

CASE STUDY: SAVINGS

US 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. By creating a policy that allowed access to only work-related sites and apps, it substantially reduced 4G consumption, as well as eliminating 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 without disrupting the morale of the workforce.

Challenges and considerations

THE ARCHITECTURE

Unlike desktop or laptop devices, which predominantly connect to the internet via known Wi-Fi and corporate infrastructure, mobile devices are much more complex. They are more ‘promiscuous’, connecting to many more known and unknown Wi-Fi networks. They use their cellular interface, a connection interface that most companies have no control over.

Mobile devices offer many options for accessing information. Users may choose the default web browser, one of many browsers provided by third parties within apps, or apps specifically designed for accessing proprietary content. The different mobile platforms and operating systems available should also be considered, where each implementation of an app can vary. In moving from the desktop to the mobile, the way users access network services, internet services and data have shifted from the existing “browser-centric” model to an “app-centric” model.

Instead of relying predominantly on a single web browser, apps that provide a cleaner, simpler and faster experience dominate on the mobile device.

Companies tackled the mobility issues raised on laptops by the use of Virtual Private Networks (VPNs). Configuring VPNs on a relatively homogeneous fleet of laptops is reasonably straight forward when compared to implementing a similar solution on mobile devices.

However, app interoperability with VPNs is a major issue for many companies. As end-users select and use a wide range of apps, each catering to their own particular tastes and use cases - combined with a small set of enterprise-specific apps - there is a vast quantity of different implementations that must be friendly.

In a world where anyone can write an app and most apps are designed for consumers rather than for the enterprise, VPNs regularly fail to adequately support many applications. When the different platform implementations of VPNS is added to the mix, the configuration interoperability quickly presents yet new challenges. This quickly becomes a headache for end users who must suffer broken apps, dwindling battery lives and slow connections. This burden is then shared with company help desks, as employees begin to complain and try to work around the enterprise configurations.

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 (for example performance and battery life). The device must also continue to perform so that it can meet the business use case for which it was originally purchased.

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 negate the benefits of Content Filtering 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.

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, where it was possible to use isolated tools to monitor employees (for example Next-Generation Firewalls and Web Filtering Gateway). On mobile devices, a mobile-first solution is essential. A solution that blends on-device and 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.

Summary

Content Filtering on mobile devices is shifting from a should-have to a must-have. With mobile usage increasing, now is the time to dedicate the same level of scrutiny and resource to managing mobile devices as desktop computers have received for decades.

Wandera's web gateway for mobile provides best-in-class Content Filtering functionality, allowing admins to control access to a large number of sites and apps using an intuitive dashboard.

As demonstrated in this white paper, Content Filtering can be applied to a range of challenges across the organization. Wandera's solution has been designed to meet these challenges, providing enterprise-grade security on a proactive and highly visible level.

These features can also be used to enhance employee productivity, to tackle obscure and expensive data costs, and to protect companies from legal liability and corporate risk.

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

wandera.com/demo

ABOUT THE AUTHOR

David Rankine oversees the Data Management and Content Filtering product lines for Wandera, the world leader in Enterprise Mobility. In this role, David works closely with Wandera's partners and sales organization to ensure the product strategy is defined and successfully executed. David is responsible for the end-to-end product line delivery process, which includes overseeing feature definition and rollout, product marketing and ongoing capability support.

David has worked in a variety of technical product roles and has experience across multiple industries. Prior to life as a Product Manager at Wandera, he was a Technical Consultant at IBM where he worked on a portfolio of complex systems integration projects.

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.