TRUST IN
GERMAN
SICHERHEIT

G DATA
WhitePaper

Mobile Device Management

G DATA Application Development

WhitePaper_MDM_2015_04_21

Contents

1. Introduction

Traditionally, enterprise network and system administrators have always managed homogenous groups of client devices. The process of planning and provisioning network clients almost exclusively dealt with desktop computers. This predictability simplified deployment of network infrastructure, client hardware and applications, ensuring uniformity across all network devices. However, since smartphones and tablets have taken the world of consumer electronics by storm, the technology landscape has become a lot more complicated. Trends like the Consumerization of IT and Bring your own device have introduced device diversity to the enterprise. Administrators are left with the task of providing broad access to resources while guaranteeing security. This whitepaper aims to outline trends in the use of smartphones and tablets in enterprise networks (chapter 2) as well as practical management strategies for administrators dealing with increased mobile device usage (chapter 3). To find out more about how G Data implements mobile device management, visit our website to download G Data TechPaper #0273.

2. Mobile devices in the enterprise

The rate of technology adoption in enterprise environments is significantly slower than the rate at which consumers embrace new devices. Even if a product can be easily incorporated in workflows, it has to be tested for compatibility issues with the corporate infrastructure – a process which can be very budget- and time-demanding. Ever since Apple popularized the mobile device category with the iPhone and iPad product launches, hundreds of millions of home and corporate users alike have gotten hooked on the combination of advanced technology and ease-of-use. However, many corporations are still struggling to properly integrate these devices into the enterprise environment. This delay in adoption often leads to tension between end users' expectations and the functionality that currently deployed enterprise solutions can offer. Two major trends in enterprise IT cover illustrate this conundrum: Consumerization of IT and Bring your own device (BYOD).

Dubbed Consumerization of IT, the influence of privately used consumer devices on enterprise IT solutions has grown immensely. End users have gotten used to permanently available mobile internet, cloud-based messaging and e-mail, as well as huge quantities of apps to customize the mobile experience. Although no administrator would deny that the use of these services can be very convenient, some of the advantages are inherently at odds with enterprise IT structures. The rate at which new apps are release for mobile platforms far exceeds the capabilities of administrators to test individual apps for compatibility and security. The use of cloud services often means storing data on servers that are managed by third parties. Even though end users have come to expect such services from their devices, not all enterprises are technically ready to offer them in a way which meets IT policies.

Even when mobile devices and services are not being actively deployed in an enterprise environment, that does not mean administrators do not encounter them at all. This trend is called Bring your own device (BYOD): end users bring their own devices to work and expect to be able to use company infrastructure, such as Wi-Fi access and network shares. Similarly, many e-mail server configurations allow remote access using mobile devices, regardless of whether that device is managed or not. BYOD often leads to knee-jerk reactions: to make sure that no sensitive data is leaked or malicious software enters the network, mobile devices are blocked from the enterprise infrastructure altogether or device functionality is severely limited by oppressive policies.

However disruptive it may sound, it is important to realize that enterprise mobile device usage is not a black-or-white phenomenon. BYOD and Consumerization of IT may seem to destabilize a perfectly organized environment, but there are several benefits to deploying corporate devices or managing

private ones. Using a device management solution can help take advantage of the positive sides of mobile device usage while limiting its effects on the rest of the enterprise infrastructure.

2.1. Benefits

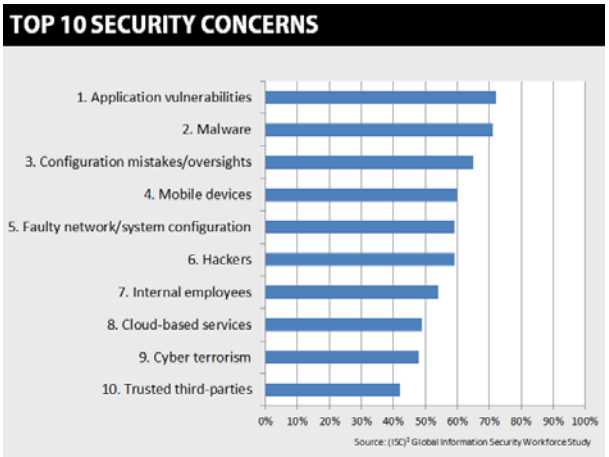
The integration of smartphones and tablets in enterprise workflows has obvious advantages, regardless of whether they are centrally deployed or brought in by employees. Offering mobile access to enterprise resources can greatly improve productivity for remote workers and contractors. A combination of access controls and device management enables safe and effective use of their device to access company resources while outside the office. Traveling no longer means a lack of communication: employees can remotely keep track of e-mail, calendar and notifications.

Enterprise devices and applications often have a higher barrier to entry with regards to usability, whereas consumer technology has often been engineered to provide a level of familiarity to end users. This reduces the learning curve for employees, allowing them to quickly get used to company issued devices.

Finally, in a BYOD environment, enterprises save money by not having to heavily invest in device deployment. Instead of buying and deploying new smartphones and tablets, employee devices can be provisioned with device management software and directly used for corporate purposes. Companies are also no longer responsible for replacement devices in case an employee loses or breaks a smartphone or tablet.

2.2. Risks

Even though mobile device adoption can have many positive effects on enterprise productivity, there are some challenges. Mobile devices were listed the fourth highest security concern in the 2015 Global Information Security Workforce Study of the (ISC)2 Foundation[1]. As with PCs, mobile devices are susceptible to malware. Especially Android and iOS are at risk: with a combined market share of 96.3 percent[2], they are a prime target for criminals. In 2014, G Data security experts investigated over 1.5 million new Android malware samples, a 30 percent increase compared to 2013[3]. Android malware is used for a variety of nefarious purposes, including:



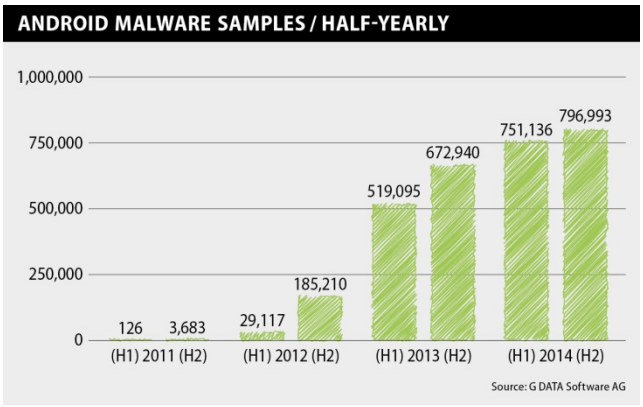
- Stealing data, such as e-mails, login data and sensitive documents.
- Causing excessive costs by sending SMS messages to (foreign) premium phone numbers
- Spying on mobile banking apps
- Locking devices in order to extract a ransom (ransomware)

However, malware is not the only threat to mobile devices. When browsing the internet, phishing websites may try to convince the user to enter personal data into a seemingly innocuous form. And even if the device itself is safe, that does not mean it can be safely used within corporate contexts. When employees use mobile devices to access corporate documents, it needs to be made sure that sensitive

[1] Source: (ISC)2 Foundation, https://www.isc2cares.org/IndustryResearch/GISWS/
[2] CY14. Source: IDC, https://www.idc.com/getdoc.jsp?containerId=prUS25450615
[3] Source: G DATA Mobile Malware Report H2/2014

information does not leak, either by accident (for example: by uploading it to a file-sharing service) or on purpose (insider threat).

In addition to security risks, mobile devices may also cause a productivity hit. The use of apps should be restricted to make sure that employees do not spend an excessive amount of time on games or other pastimes. Contact management can help lock down use of the telephone functionality to the absolutely necessary, saving time and costs.



The benefits of mobile device usage in the enterprise outweigh the risks. However, the latter still need to be mitigated. An integrated mobile device management policy can help manage security risks as well as productivity issues and ensures safe and efficient use of smartphones and tablets.

3. Mobile device management

As an administrator, ignoring consumerization and BYOD is near impossible. End users will continue to demand enterprise smartphones and tablets that adhere to the usability paradigm they have gotten used to. If such devices are not being actively deployed, they will bring their own. Considering the advantages mobile devices can bring to productivity, the goal of mobile device management should be to maximize productivity while guaranteeing security and minimizing costs.

3.1. Deployment and administration

Before smartphones or tablets can be managed by a mobile device management solution, they have to be deployed. Deployment involves a one-time initial connection between device and server, after which the device will periodically report back to the server and can be remotely managed. Communication between server and device takes place in the form of internet traffic (when a direct connection to the server can be established), push messages (often based on vendor-specific cloud messaging solutions) or SMS messages (when no mobile internet connection is available). A permanent connection between device and server is not required: the device can carry out server policies even if there is no contact to the server. This means that devices are protected at all times, even outside the enterprise environment.

Deployment should be streamlined as much as possible. New, company-managed devices should always be equipped with mobile device management features before being handed over to employees. BYOD devices should be denied access to the corporate network and its resources until they have been equipped with mobile device management. Optionally, a guest network can be used for devices that do not meet the requirements or are used by visitors.

To avoid an increased workload, administrators should choose a device management solution that integrates with existing management structures. The use of multiple back-ends should be avoided. Ideally, mobile devices can be managed using the same kind of interface and reporting capabilities that are available for other device types in the network, in order to support an integrated workflow and consistent configuration.

For BYOD devices, the legal aspect of device management should be considered. Because this type of devices is not company property, administrators do not automatically have the right to manage it. Especially permissions like remote wipe can be controversial. Depending on the legal situation, companies may have to ask permission from the end user before enrolling a device in mobile device management. It is recommended to define an end user license agreement (EULA) that explains the actions that the company needs to be able to execute on the device. The end user can either accept or decline the agreement, but access to corporate resources will not be available if the EULA is declined. Even for non-BYOD devices, a EULA can be useful.

3.2. Anti-theft

Mobile devices increase risk levels for the physical infrastructure and information-based workflows. Between employees bringing sensitive files with them on the road and mobile devices getting lost or stolen, it is easier than ever to accidentally leak confidential information. To make sure that corporate e-mails, documents and other communication cannot be accessed when a device is lost or stolen, several measures can be defined. Firstly, it can be helpful to try to recover the device. Locating it using GPS technology or triggering an alarm sound can help. If locating the device is not an option or does not yield any usable results, locking it will make the device useless. As a last measure, devices can be reset to the factory defaults, wiping all data on the device.

3.3. Apps

Part of the charm of mobile devices is the fact that their default functionality can be expanded by installing apps. Even in a corporate context, this can be extremely useful: productivity tools or configuration apps can significantly increase the amount of use cases for mobile devices. At the same time, corporate devices should provide a controlled environment, making sure that apps cannot cause compatibility problems, leak sensitive information, or spread malware. App management is a powerful way to control the functionality of a mobile device, balancing security with usability.

Separating the good apps from the bad can be a difficult task. Some apps are clearly unsuitable for corporate environments, such as games. Others may serve some purpose, but can possibly harbor privacy risks, such as online file storage services. Even apps that seem risk-free may later turn out to be compromised, either because the app itself contains security flaws, because its backend services are compromised, or because it insecurely transmits information. Productivity is also a factor: for example, employees that only need a smartphone in order to call and make appointments, would only get access to phone and calendar components, while employees that are working on documents on the road get access to browser, office apps and other required components.

3.4. Real-time and on demand protection

Like desktop and laptop clients, mobile clients are also vulnerable to online attacks. Rooted Android devices in particular do not have sufficient protection mechanisms against malicious apps from unknown sources, but even malevolent apps that manage to sneak their way into the official app stores can have severe implications. Similarly, websites may try to serve malware, take advantage of vulnerabilities in the operating system or otherwise deceive the end user. As on desktop computers, phishing websites may try to coax users into handing over passwords or other sensitive data. To counter these threats, protection measures should be configured for all managed mobile devices.

Real-time protection protects devices all the time without requiring user interaction. This includes technologies like phishing protection and automatic virus checks. On demand protection, on the other hand, is only activated once an end user or administrator triggers it. For example, a virus check can be manually initiated to make sure that no malicious apps have been previously installed on the device.

Real-time and on demand protection solutions differ greatly per client platform. Whereas Android clients are especially susceptible to malicious apps, iOS devices are more vulnerable to data loss or phishing threats. Mobile device management solutions should offer measures to optimally suit each mobile platform: a one size fits all module does not do justice to the wide range of threats that devices face.

3.5. Contact management and filtering

For devices that are used in a corporate context, controlling communication streams can be essential. Blocking apps can help if communication should be entirely prevented, but in some scenarios a more fine-grained filter should be deployed. Rather than completely blocking the Phone app if a device is only meant to be used for work-related communication, outgoing and incoming calls could be filtered if they do not meet corporate criteria. For example, a company that supplies its employees with phones to communicate with headquarters while on the road could block all phone calls except those with pre-approved corporate contacts.

Central to contact management is a managed phone book. Contacts stored on the device can be synchronized to the central server and administrators can push the latest phone numbers to devices. Like app management, contact management can be used for individual devices, but is best combined with group-based management. Individual phone numbers can be allowed or blocked for groups of devices at once or a complete corporate phone book can be pushed to all devices.

To find out more about how G Data implements mobile device management, visit our website to download G Data TechPaper #0273.