tori

experience. the difference.

Transform your Enterprise with Mobility

Integrating Mobile Application Development with Mobile Device Management Tools

Integrating Mobile Application Development with Mobile Device Management Tools

By Costas Liassides, TORI Global

Introduction

Currently there are over 6 billion mobile subscriptions globally, (Sanou, 2011), and growing. Mobile technology is a booming business and will continue to excel. IT organizations have been and continue to jump onboard – not only with Bring your own device, (BYOD), solutions & strategies for the enterprise, but also for the increase in demand of mobile applications. ITunes App Store alone has 1.2 million, (Statista, 2015), apps available for purchase/free download. Android app store has even more with the current number sitting at just over 1.3 million, (Statista, 2015), apps available for purchase/free download. This staggering number has arisen over the last 9 year period, since the first true introduction of the "smartphone" by Apple Inc. and Samsung.

There are many advantages to mobile application development & engineering. Custom specific application can provide company specific and targeted ways to improve business productivity and customer engagement, provide better customer service and help organisations differentiate themselves from the competition. Also, some companies internally develop their own mobile applications as they are not able to control mobile devices and their commercially available applications or native operating systems, (OS's), as tightly as necessary. However, if an organisation creates their own mobile applications, they have the freedom to design and implement their own controls to meet the firm's requirement.

But how can IT – already struggling with the challenges of managing an increasingly mobile infrastructure with ever-growing diversity and complexity – ensure the security of mobile devices and applications during the critical development phase? Beta/proof of concept mobile application versions are typically distributed to employees' mobile phones during the testing phase, adding layers of risk and complexity to the development process. Beta applications must be kept confidential – to avoid theft of intellectual property and to prevent early, unfinished versions leaking to the public.

In addressing most of these issues, most IT organisations use completely separate mobile application development and mobile device management tools – which can leave significant gaps in device and application security. This white paper addresses the challenges of managing mobile devices and the security gaps that can occur in the mobile application development process. It will then discuss the advantages of using integrated technologies for mobile application development and mobile device management, rather than independent solutions to take on the challenges – and opportunities – of BYOD and mobile application development environments.

Addressing the challenges of managing mobile applications and devices

While the widespread business use of mobile devices has enabled new levels of productivity and flexibility in the workplace, it has also introduced new changes and challenges related to IT management and security – significantly disrupting traditional management paradigms.

As a result of these shifts, (especially the move to employee owned devices from the company provided equipment), it is very difficult for IT to maintain control over the organizational owned data, applications and relevant upgrades. With the rise of BYOD usage, the power had now shifted to the mobile device user, raising serious concerns in mobile application development environments, where the security of in-process enterprise applications is a risk.

Limitations of native OS technologies

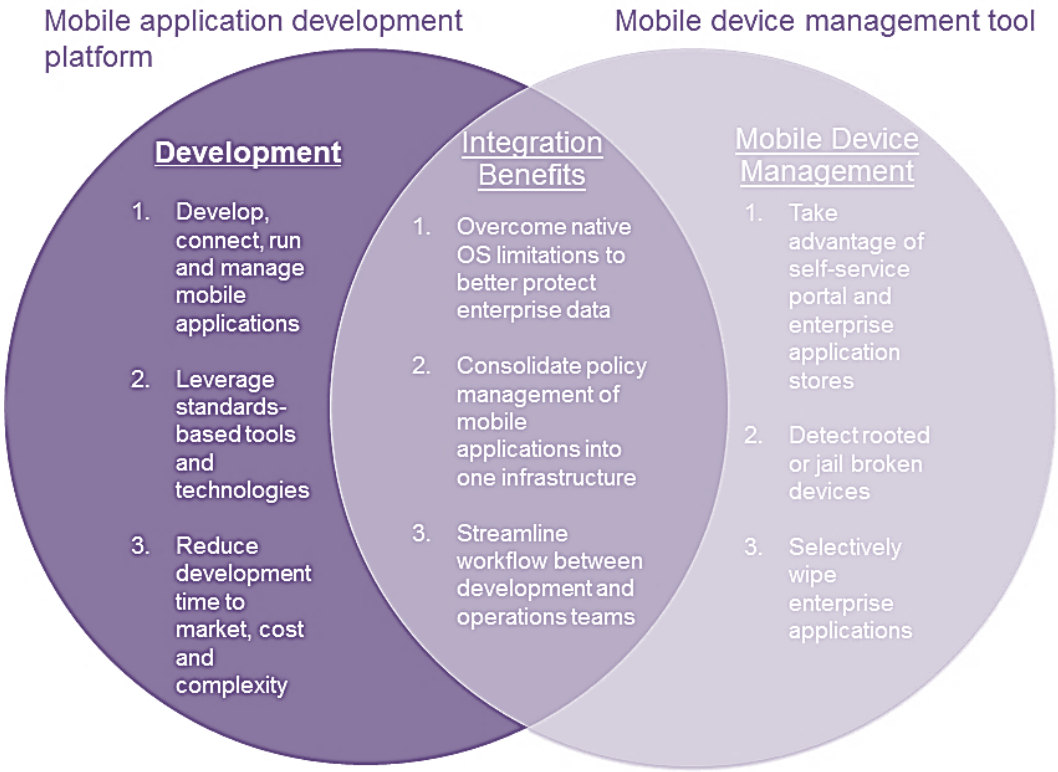
In any environment, it is difficult for any IT organisation to safeguard enterprise application data on mobile devices due to the management limitations of OS's such as Google Android and Apple iOS. This represents a sharp contrast to traditional computing scenarios, where IT could easily wipe corporate data from desktops when employees left the organisation or were out compliance with the company policy. Control is especially critical in mobile environments, where the risk of application data leakage is higher. That's because in the mobile realm, native OS technologies prioritize the user experience over IT control – and many don't allow IT to selectively wipe application data from mobile devices. In fact, these native OS's often prevent the enterprise application from detecting whether the mobile device on which it is installed is in or out of compliance.

This lack of control leaves a marked security gap wide open. What if, for example, an employee with multiple enterprise applications on an Android device violates corporate policy, putting enterprise data at risk? IT would need to temporarily deny access to or remotely remove the enterprise applications from the device, as well as wipe it clean of application data. But since the Android OS does not enable IT to forcibly install or uninstall applications or control them remotely, the enterprise applications would remain at high risk. Also, what if the applications in question are currently in the testing phase of deployment? Their early release could have a major negative effect to the organisation in terms of financial and intellectual property losses.

Limitations of using independent development and management tools

On today's technological planet, where instrumented, interconnected and intelligent businesses collect, process, use and store more information than ever before, organisations must invest in tools to secure and manage the gamut of devices used by employees. The right mobile device management solution can enable unified management of all enterprise devices, from desktops to laptops to smartphones, and more. However, when mobile devices are used in the development process – as they must be to test new mobile applications – management and security shortcomings occur. Applications in development can be placed at risk because most mobile device management solutions don't integrate with mobile application development platforms.

A common response for many organisations is to use device management tools that are independent of the development tools with which they build mobile applications. However, this option leaves organisations in need of a way to deal with the associated security gaps. Connecting the development and management functions can help your organisation overcome these known limitations.



There are clear benefits to mobile application development with mobile device management

Integrating mobile development and management technologies

There is known value to be gained from integrating mobile application development with mobile device management. Organisations can better protect enterprise data during development by consolidating the policy management of mobile applications into a single infrastructure. Integrating these tools also can help streamline the work-flow between development and operational teams.

Consolidate mobile application policy management

Integrating the two technologies can help overcome many native OS management limitations. For one thing, this integration enables a mobiles application to periodically “check in” with the endpoint management tool to provide the compliance state of the user and the device. IT can then deny mobile enterprise application access if the mobile device is found to be out of compliance with policy.

By integrating their endpoint management tools and mobile application development platforms, administrators can manage policies of all applications built using the mobile application development platform and tested using mobile devices. They can then avoid the need to set some device level policies in the endpoint management tool – and separately manage application specific policies using the mobile application development platform.

Integrating mobile device management with mobile application development also enables organisations to streamline corporate policies across development and operations – since mandatory security and compliance approval processes can be complex and time consuming. For example, integration enables a portfolio of applications developed on a mobile application development platform to go through a uniform approval and compliance checklist, enforced by centralised security group, during the testing phase. In addition, application developers can receive iterative feedback from other stakeholders on application policy, compliance and security considerations. The security group can then preapprove these applications in the production stage in a much shorter timeframe. This, in turn, can reduce the length of application release cycles, as development groups become independent of implementing or enforcing policies one application at a time.

Streamline application development work-flow

Integrating development and management functions also streamlines the mobile application development work-flow – which further contributes to an organisation's ability to deploy custom built applications more quickly. They can move applications more smoothly through the deployment process – from development through quality assurance, then on to employee mobile devices for internal testing, during which the applications can be tightly managed, before they ultimately land in the end user's hands.

In addition, integration can provide a greater degree of security and quality during the development process. For example, using a mobile device management tool with an application deployment platform can help developers feel more confident that they are using the right application version, one that hasn't been corrupted or manipulated in some way between the development and the production stages. It gives the team more control over pulling the application out of testing for adjustments, updating it later or remove it completely from circulation, as needed.

Choosing a strong mobile foundation

There are various mobile device management tools currently available in the marketplace. Some example are:

AirWatch® Mobile Device Management enables businesses to address challenges associated with mobility by providing a simplified, efficient way to view and manage all devices from the central admin console. Our solution enables you to enroll devices in your enterprise environment quickly, configure and update device settings over-the-air, and secure mobile devices. With AirWatch, you can manage a diverse fleet of Android, Apple iOS, BlackBerry, Mac OS, Symbian, Windows

Mobile, Windows PC/RT and Windows Phone devices from a single management console. (VMWARE, 2015)

IBM® MobileFirst Platform Foundation, helps enterprises deliver on their mobile strategy. It provides an open and comprehensive platform to not only build, but test, run and manage native, hybrid and mobile web apps. Available as an on premises or private cloud solution, IBM MobileFirst Foundation can help reduce both application development and maintenance costs, improve time-to-market and enhance mobile application governance and security. (IBM, 2015)

Conclusion

The comprehensive set of mobile capabilities available from VMWARE and IBM helps organisations increase efficiencies and gain a competitive advantage. In, particular the ability to integrate mobile applications with a mobile device management tool delivers an advanced array of connectivity and management capabilities to support and protect the wide variety of mobile devices and mobile application types that are increasingly common in today's technological driven environment.

References

IBM. (2015). IBM MobileFirst. Retrieved from IBM MobileFirst: http://www-03.ibm.com/software/products/en/mobilefirstfoundation
Sanou, B. (2011). International Telecommunication Union - Measuring the Information Society. Retrieved from International Telecommunication Union: http://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-ICTOI-2012-SUM-PDF-E.pdf
Statista. (2015). Statista. Retrieved from Statista: http://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/
VMWARE. (2015). Airwatch. Retrieved from Airwatch: http://www.air-watch.com/solutions/mobile-device-management/?cid=70150000000p2j9