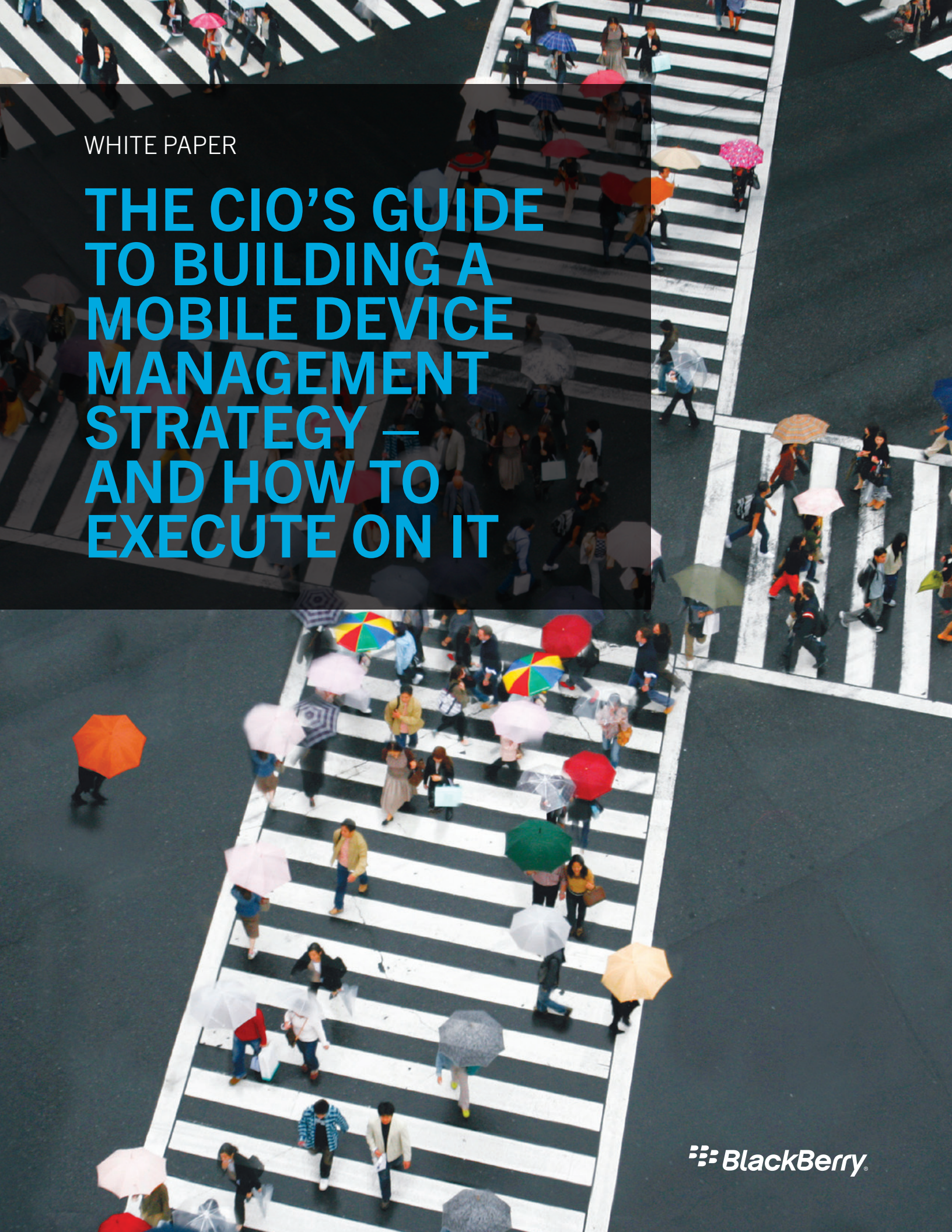

WHITE PAPER

THE CIO'S GUIDE TO BUILDING A MOBILE DEVICE MANAGEMENT STRATEGY — AND HOW TO EXECUTE ON IT

BlackBerry

Executive Summary

The explosive growth of worker mobility is driving the rapid adoption of mobile devices within the enterprise. Today's smartphones and tablet computers are as powerful and capable as the enterprise desktop computers five to ten years previously. More and more workers are using smartphones and tablets to do their work regardless of time and place. However, the proliferation of mobile devices within the enterprise does not come without risk. Managing these devices in the field can be difficult. As they are prone to loss and theft, security is more important than ever. Enterprise Mobile Device Management (MDM) solutions are the answer to many of the issues caused by the rapid growth of smartphones and tablets. MDM provides IT with a complete set of inventory, control, and reporting tools that make it easy to manage mobile devices wherever they are. Gartner found that MDM solutions can reduce the total cost of ownership (TCO) of mobile devices by over 50%.

Another issue that many companies are coming to grips with is the consumerization of smartphones and tablet computers into the enterprise. Over the last few years there has been a steady growth in the number of employee-liable devices that enterprise IT is required to manage. This task is made extremely challenging by the various makes and models of devices, different operating systems, and different device firmware revisions. Research In Motion® (RIM®) understands the challenge that employee-liable devices present to the enterprise, and in response, has released new products to help enterprise IT. BlackBerry® Mobile Fusion will simplify the management of smartphones and tablets running BlackBerry®, Google® Android®, and Apple® iOS® operating systems. BlackBerry Mobile Fusion extends the best-in-class BlackBerry device management tools that IT is familiar with to devices from other manufacturers. BlackBerry® Balance™ technology will help keep personal and work information separate, allowing workers to enjoy their BlackBerry smartphone or tablet without compromise. With the release of these innovative products, RIM once again shows their understanding of the enterprise mobility market.

Table of Contents

BlackBerry

Introduction

The incredible success of mobile communications is plain to see – anywhere you go, people of all ages are talking, texting, and playing on mobile devices. According to the International Telecommunications Union (ITU), almost 80% of the world's population has a cell phone, and in many emerging markets, the number of mobile lines is more than twice the number of fixed lines. In the enterprise, worker mobility has been increasing for years. This trend has helped drive the evolution of the enterprise computing platform from fixed PCs (desktops), through portable computers (laptops and netbooks) to mobile devices (smartphones and tablets). Today, the mobile worker can use their smartphone and tablet to remain connected and productive throughout the day from virtually anywhere.

Smartphones and tablets offer comprehensive communications features and can run many of the applications that mobile workers are asking for such as email, calendaring, instant messaging, and strategic Line-of-Business (LOB) applications. These mobile devices can boost worker productivity while enhancing their quality of life. Smartphones were first popular in the enterprise, but due to falling prices and improved usability they have exploded into the consumer market. Ironically, their popularity in the consumer market is driving increased penetration back into the enterprise as workers purchase their own smartphones and bring them to work. IDC predicts that by 2015, almost 55 percent of corporate mobile devices will be employee-liable devices.[1] This trend is likely to be echoed with tablet computers. While it is true that employee-liable devices are becoming more popular, many CIO's and network administrators have concerns. In late 2010, RIM surveyed over 150 executives to discover their opinions and concerns about mobile devices. A key finding was that of the executives surveyed, 84% responded that the security and management of employee-liable devices was a significant concern.

Another area of concern for many companies is the TCO of the devices supporting business mobility – acquisition cost and mobile network charges are just a small part of the total costs. Companies also have to manage their mobile devices – replace lost or stolen devices, deploy firmware and software updates, and secure mobile devices in the field. This already difficult task is becoming more costly and complicated as new smartphones are introduced into the marketplace, purchased, and brought to work by employees. According to Forrester Research, over 60% of US and European companies surveyed support, or plan to support multiple smartphone OS's.[2] Unfortunately, many companies that are supporting or planning to support employee-liable devices are doing so without a complete understanding of the risks and costs associated with this decision, or without the knowledge to make it happen.

[1] Source: Worldwide Business Use Smartphone 2011-2015 Forecast and Analysis (IDC# 230311, September 2011)
[2] Forrester Consulting, May 2009 - Understanding The Critical Role Of Device Management And Security In Your Business Mobile Strategy

The Enterprise Mobility Strategy

The steady growth in worker mobility is convincing many companies to develop an Enterprise Mobility Strategy. The importance of mobility planning continues to grow as corporate spending on wireless and mobility products and services is rapidly becoming a major component of the annual IT budget. For many companies, wireless voice and data spending has overtaken wired voice and data spending as a portion of the annual telecom budget. The Enterprise Mobility Strategy demonstrates the company's commitment to enterprise mobility. The goal of this is to align mobile IT priorities with short-term and long-term business goals. It should be a formal document created by IT, HR, and Legal, but must include input from all stakeholders. The Enterprise Mobility strategy answers important questions such as:

- Which employees get what type of mobile device, i.e. feature phone, smartphone and/or tablet?
- How much security is required and how will it be enforced?
- What data, applications, and functions are allowed on enterprise devices?
- Who supports the mobile device users and manages the devices?
- Who pays for hardware, software, and wireless services?
- Are employee-liable devices supported, and if so, how?

The Enterprise Mobility Strategy lists and describes the company's key mobility policies. It also provides a valuable starting point for the company's Wireless Security Strategy. This strategy extends the company's 'wired' security to include policies for user authentication, network security, and malware protection for mobile workers accessing the company network over a wireless connection. For more information about wireless security, visit blackberry.com/security.

After the Enterprise Mobility Strategy is developed, employees must be educated. All company employees should be trained on and have access to the latest version of the document on the company intranet. However, training may not be enough to ensure that these policies are respected. Even the best employees take shortcuts and/or do not think that they are ever going to lose their device. In addition, someone must be responsible to audit compliance and make sure that the policies are enforced. This function can be very expensive when the number of mobile workers in a company grows. To make this job easier, and to reduce the TCO of mobile devices, more and more companies are deploying Mobile Device Management (MDM) solutions.

Mobile Device Management

Mobile Device Management solutions are the most effective tool for a company to implement and enforce an Enterprise Mobility Strategy or Wireless Security Strategy. Most MDM solutions employ user-defined 'rules' mapped to specific policies within these strategy documents. When properly deployed, MDM solutions allow IT administrators to manage smartphones and tablets similar to the way that they manage conventional IT assets such as desktop and laptop computers. They automate important IT tasks such as mobile device asset management, device configuration, firmware/software distribution, and backing up and restoring device information. MDM can become very challenging in corporate environments that support employee liable phones. Each make and model of phone may support a different degree of MDM.

ASSET MANAGEMENT

Given the speed at which wireless technology is changing and new mobile devices are being introduced into the market, the simple task of determining whom within your organization is using what kind of mobile device can be challenging. It is made even more difficult by the progress of employee-liable devices. However, this inventory stage is one of the most essential elements for a successful MDM strategy. It is critical that IT knows who is using what make and model of mobile device, what operating system, version, and what firmware release are being used; and what applications are installed on every mobile device that is accessing the corporate network. The inventory must include all types of mobile devices; feature phones, smartphones, and tablet computers. Without this basic information, effective MDM and reliable wireless security are not achievable.

The asset inventory phase is an excellent opportunity to begin the segmenting and profiling of mobile users that was defined within the Enterprise Mobility Strategy. Determining whom in the organization needs a mobile device for what purpose allows IT to segment and categorize mobile devices by job function, mobility requirements, geographic location, device type/class or any other criteria. This categorization is a powerful enabler for Mobile Device Management. Instead of specific users, IT staff can use the categorization to configure security profiles, device settings, and application suites.

OVER-THE-AIR (OTA) FEATURES

Since mobile workers spend so much of their time away from the office, one of the most important requirements for any MDM solution is comprehensive over-the-air capabilities. OTA allows IT real-time management of mobile devices no matter where they are, or what time of day it is. OTA for mobile devices is also important since they tend to be replaced more often than laptops and desktops; an average of 18 months as opposed to three years. An MDM solution's OTA features can significantly reduce enterprise mobile device TCO. Important OTA features include; configuration management, backup/restore, and mobile application deployment.

Mobile Device Management

Configuration Management

Remote setup and configuration of mobile devices is an essential element of MDM. It allows IT staff to configure new devices quickly and easily without resorting to a USB cable and tethering the configuration information onto the device. Remote configuration from a central MDM solution enables IT staff to manage a number of different parameters including:

- Connection parameters for wireless networks (WiFi or 2G/3G/4G public mobile networks).
- Enabling/disabling hardware capabilities such as GPS, camera, or Bluetooth.
- Settings for email, messaging, and web browsing (proxy information).

Central control and automatic configuration of the mobile device becomes even more important as more and more employee-liable devices appear in the enterprise. It is difficult for IT staff to become experts on every mobile device and every operating system version in the marketplace, whereas a high-quality enterprise MDM solution will support many different makes and models of mobile devices.

Backup/Restore

Due to their small size, mobile devices are prone to theft and loss. For an idea of scale, recent market research includes the following;

- A survey from Norton by Symantec (NASDAQ: SYMC) reveals that 36 percent of consumers in the U.S. have fallen victim to cell phone loss or theft.
- A 2010 report from the BBC reported than 228 phones in the UK are stolen every hour.
- 'Alarming Statistics' from MicroTrax indicate that 113 cell phones are lost or stolen every minute in the U.S.

Whichever set of numbers you believe, it is clear that every year hundreds of thousands of mobile devices are lost or stolen. Backup and restore are essential OTA features for dealing with lost, stolen, or damaged mobile devices. Automatic backup and restore of mobile device settings, data, and applications is also valuable for new and replacement devices, a common occurrence given the 18 to 24 month lifecycle of many enterprise smartphones. It can also be used to synchronize important files between a mobile worker's desktop computer and their mobile device.

Software & Firmware Distribution and Updating

As mentioned previously, an Enterprise Mobility Strategy defines categories of users based on their mobility requirements. An important aspect of these requirements is what mobile applications are required for the user to do their work. For example, does the mobile worker only require access to horizontal applications such as email, messaging, and calendaring? Does the user require any off-the-shelf productivity applications or more specialized mobile Line-of-Business (LOB) applications? Is the user allowed to download personal applications for productivity or entertainment? An MDM solution maintains an index of what applications are appropriate for which users for automatic distribution. MDM can also make it easy for IT Staff to track how software licenses are deployed and used. In addition, an MDM solution can maintain the version of the application and automatically download updates in a bandwidth efficient format, a 'delta' of the changes as opposed to a complete application download and install.

Mobile Device Management

An MDM solution can maintain more than just application lists and updates. It can manage lower level code such as operating system updates and even firmware updates for a mobile device. It can also automatically add, modify and delete important user content. Any document and file type can be managed at the byte-level, including price lists, address books, reference materials, and brochures. The most important thing is that applications and content can be electronically distributed, installed, and maintained – all without the mobile worker's knowledge or involvement. Using MDM, IT staff can easily manage the application lists and content requirements without ever having to touch or tether a mobile device.

MOBILE SECURITY ENFORCEMENT

Mobile Device Management is the most effective way to enforce a company's Wireless Security Strategy. Mobile devices present a significant security risk for many organizations. These devices can hold sensitive corporate data and are easily lost or stolen. Company information that is stored on a mobile device must be just as secure as information stored behind the firewall on the corporate network. Unauthorized access to corporate data can cause bad press and embarrassment, or equally likely, financial loss or litigation. To mitigate this risk, IT staff should have the ability to control all aspects of mobile device security. This includes the ability to mandate passwords for mobile device users, encrypt data stores, and erase data from mobile devices remotely.

Authentication

Mobile device authentication and mandatory passwords are the easiest, most effective MDM policies to enforce. If/when, a mobile device is lost or stolen, the device should not be usable by anyone other than the owner, and the data on the device needs to remain secure. IT staff should force mobile devices to adhere to a defined password policy. All mobile devices should have an inactivity lock and be protected by a strong power-on password that is refreshed every three to six months. Good MDM solutions provide a complete set of password functions to secure mobile devices.

Remote Locking/Wiping

Another important mobile security element is the ability to remotely lock and/or wipe a mobile device that has been lost or stolen. This feature prevents access to any sensitive data on the device, but it can also prevent unauthorized access to the corporate network. It is important that mobile workers are trained to report a lost or stolen mobile device as soon as possible. Even a brief delay can have serious implications for the company. If the mobile device is returned, the OTA restore and remote configuration features of an MDM solution can quickly re-configure the device back to its natural operating state.

Encryption

Despite the best intentions of even the most contentious of users, remote locking/wiping of a missing mobile device is not the only way to prevent unauthorized access to device data. Depending on the role of the mobile worker, it may be appropriate to encrypt data on the device. File level, application level, or even full disk encryption can protect sensitive data in the event of a lost or stolen mobile device. Encryption must extend to both the device and any removable data storage. Most MDM solutions will allow IT staff to select what data to encrypt for each individual user or user category.

Mobile Device Management

Virus and other Malware Protection

There is no question that mobile applications can increase the productivity of mobile workers; however, what applications are installed on a mobile device and how they are sourced and deployed is a serious concern for the enterprise. It is easy for viruses, trojans, worms, and other malware to be unknowingly loaded onto wireless devices. Malware threatens information confidentiality, endangers system passwords, and increases the risk of data loss or compromise.

Mobile Device Management provides a number of different ways to prevent the download of malware. One common approach for preventing the transmission and proliferation of malware on mobile devices is to install virtual real-time anti-virus scanning software. This software is designed to detect and contain malware. It is easy for MDM solutions to mandate anti-virus software and keep it up to date. Another more draconian approach is for IT staff to completely disable the ability to download and install applications. While this may be the safest route, it unquestionably affects the satisfaction of the mobile device user. However, it does not have to be all or nothing – MDM can be used to restrict what types of applications are installed onto a mobile device, or control what phone features are accessible, such as:

- Specify exactly which applications – trusted, corporate-approved applications only – are permitted on the device
- Prevent third party applications from using persistent storage on the device
- Determine which resources – such as email, phone, and device encryption key and certificate-store – third party applications can access on the device
- Restrict the types of connections – such as network connections inside the firewall – that a third-party application running on the device can establish

The Next-Generation of Mobile Device Management

Robust Mobile Device Management has always been a key differentiator of the BlackBerry products. Enterprise IT staff has benefited from a comprehensive set of device management tools that have allowed them to control all of the company's BlackBerry devices. The growth of employee-liable devices into the enterprise has presented a number of challenges. New makes and models of devices, different operating systems and firmware versions make comprehensive mobile device management a challenge. In addition, employees that are purchasing and bringing their own smartphones and tablets to the office are insisting on using them for personal reasons too. There are BlackBerry products that have been created to specifically deal with these concerns.

BLACKBERRY MOBILE FUSION

BlackBerry Mobile Fusion is a new BlackBerry enterprise software platform that helps make managing mobile devices faster, easier, and more organized than ever before. BlackBerry Mobile Fusion brings together the market-leading BlackBerry® Enterprise Server management capabilities for BlackBerry smartphones with new management capabilities for BlackBerry® PlayBook™ tablets, as well as mobile device management for smartphones and tablets running Android and iOS operating systems. It helps make it easy to protect business information, keep mobile workers connected with the information they need, and provide administrators with efficient tools that help ensure the business is moving ahead.

FEATURE	BENEFIT
Support for devices that use Apple iOS and Google Android operating systems	Use BlackBerry Mobile Fusion to manage and secure devices that use Apple iOS and Google Android operating systems. It will enable administrators to add and import iOS and Android users, create group memberships, view user and device information, define IT policies and connectivity settings, manage apps on devices, and assist users in the recovery of misplaced devices.
Manage devices, users, groups, and policies from a single location	From a single interface, administrators can access the most common management tasks for mobile device management across multiple BlackBerry domains. Administrators can create and manage groups, manage user profiles, and provision mobile devices.
Manage required and optional work applications	Administrators can support over-the-air installation, upgrading and auditing of required and optional apps for BlackBerry devices. For BlackBerry PlayBook tablets, BlackBerry Mobile Fusion works with BlackBerry® App World™ to enable administrators to push and install required work apps on users' tablets. Administrators can also make a separate catalogue of optional apps available for download through the 'Work' channel of BlackBerry App World.
Security designed for everyone	A variety of policies provide maximum control with minimal impact to the user experience. For BlackBerry devices, BlackBerry Mobile Fusion leverages the security of the BlackBerry® solution to provide an added layer of protection for the synchronization of email, contacts, and calendar information.
Manage and secure BlackBerry PlayBook tablets	Features of BlackBerry Mobile Fusion enable organizations to manage and secure BlackBerry PlayBook tablets. After associating a tablet with an individual user, administrators can configure the tablet for work purposes using a centralized administrative interface. Administrators can set password requirements, enable encryption of work information, remotely lock or wipe work-related or all information from BlackBerry PlayBook tablets.

The Next-Generation of Mobile Device Management

BLACKBERRY BALANCE

As more personal devices make their way into the enterprise, CIOs and IT administrators must contend with the privacy, security, and management of employee-liable devices. BlackBerry Balance allows administrators and corporate IT to separate users' work and personal data on BlackBerry smartphones and tablets. This feature makes it easier to manage and secure employee-owned, or employee-liable, smartphones and tablets. With BlackBerry Balance, IT administrators can delete just work data or applications from an employee-owned device, without affecting any personal data, or IT admins can still perform a full wipe, if necessary. And BlackBerry Balance can be used to remove all corporate IT policies from users' smartphones. BlackBerry Balance also offers new safeguards to prevent users from copying sensitive work data into personal applications or email. Admins can prevent device backups to protect potentially sensitive data, and they can control and encrypt work data stored on a media card. Finally, organizations can use BlackBerry Balance to prevent access to corporate data via third-party applications.

Conclusion

The rapid growth of mobile workers makes an enterprise MDM solution a necessity. Almost any level of implementation will result in a positive return, but companies that develop an Enterprise Mobility Strategy and follow up with MDM can expect significantly more benefits. Gartner reported in their last TCO study for PDAs and smartphones, that a properly deployed Mobile Device Management solution could reduce mobility operational expenses by up to 49%. An enterprise MDM solution improves mobile security, reduces risk, and makes it easier for IT administrators to manage the growing number of mobile users.

BENEFIT	DESCRIPTION
Reduced Total Cost of Ownership (TCO)	Reducing mobile device TCO is perhaps the most conspicuous benefit resulting from the deployment of an MDM solution. Gartner found that managed devices have significantly lower TCO (by 53% to 63%) than unmanaged devices. Together, the centralized control and OTA capabilities of an MDM solution provide tremendous leverage to IT staff allowing them to manage multiple mobile devices simultaneously without the need to touch them. In addition, OTA configuration and application management can happen at any time of day, thus precluding the personal productivity-sapping requirement for the mobile worker to relinquish their device to IT for updating.
Improved Mobile Security	An improvement in enterprise wireless security should be the most subtle benefit from MDM. The absence of wireless security can lead to bad publicity, corporate espionage, fines, and litigation. Enforcing basic security measures such as power-on passwords and encrypted data stores is important, since only about half of mobile workers employ even these minimal security measures on their own. Using MDM to employ the complete range of wireless security rules, will significantly mitigate the risk associated with lost and stolen devices. It will also help with enterprise compliance to key industry regulations such as Sarbanes-Oxley and Health Insurance Portability and Accountability Act (HIPAA).
Improved Productivity	Managing mobile smartphones and tablets as efficiently and thoroughly as laptops and PC's attached to the network is a tremendous boon to mobile worker productivity. Troubleshooting problems no longer requires that the mobile worker make a special trip back to the office, instead, IT staff can often diagnose and repair most problems quickly and easily no matter where the mobile worker is located. In addition, the ability to OTA configuration changes, new operating system versions and application updates will reduce mobile worker downtime.

For More Information

RIM offers a number of different resources to learn more about wireless solutions in general and BlackBerry in particular. The web site blackberry.com is a good first place to start. The Technical Knowledge Center blackberry.com/support on the site can help you get answers to particular questions. To find other resources and whitepapers, visit the BlackBerry Resource Centre blackberryresourcecenter.virtualevents365.com/index.php

www.blackberry.com/business

© 2012 Research In Motion Limited. All rights reserved. BlackBerry®, RIM®, Research In Motion®, BBM™ and related trademarks, names and logos are the property of Research In Motion Limited and are registered and/or used in the U.S. and countries around the world.