



Whitepaper

September 2010

# Choosing an Enterprise-Class Wireless Operating System: A Comparison of Android, BlackBerry, iPhone and Windows Mobile

*A J.Gold Associates White Paper*

---

*“Security considerations remain the single biggest limitation to more aggressive expansion of wireless device usage in many enterprises. .... It is imperative that companies evaluate a potential device selection based on its inherent platform security capabilities, particularly around the security embedded within the device Operating System (OS)... This paper will explore some of the key criteria necessary in a mobile OS so that enterprise use of the device will not compromise the integrity of the company’s security and put it at risk for costly legal and/or governmental actions. This whitepaper will compare the attributes of three Mobile Operating Systems ... Android from Google, BlackBerry from Research in Motion, iPhone from Apple, and Windows Mobile from Microsoft”*





# Choosing an Enterprise-Class Wireless Operating System: A Comparison of Android, BlackBerry, iPhone and Windows Mobile

## Contents

<b>Introduction .....</b>	<b>3</b>
<b>Components of a Secure Mobile OS.....</b>	<b>4</b>
<i>Authentication .....</i>	<i>4</i>
➤ Android.....	4
➤ BlackBerry.....	4
➤ iPhone.....	5
➤ Windows Mobile.....	5
<i>Data Vaulting .....</i>	<i>5</i>
➤ Android.....	6
➤ BlackBerry.....	6
➤ iPhone.....	6
➤ Windows Mobile.....	6
<i>Application Verification.....</i>	<i>7</i>
➤ Android.....	7
➤ BlackBerry.....	7
➤ iPhone.....	7
➤ Windows Mobile.....	8
<i>Reliability.....</i>	<i>8</i>
➤ Android.....	9
➤ BlackBerry.....	9
➤ iPhone.....	9
➤ Windows Mobile.....	9
<i>Manageability and Policy Enforcement.....</i>	<i>9</i>
➤ Android.....	10
➤ BlackBerry.....	10
➤ iPhone.....	10
➤ Windows Mobile.....	10
<i>Tamper Resistance.....</i>	<i>11</i>
➤ Android.....	11



## Choosing an Enterprise-Class Wireless Operating System: A Comparison of Android, BlackBerry, iPhone and Windows Mobile

- BlackBerry..... 11
- iPhone..... 11
- Windows Mobile..... 12
- Security vs. Usability..... 12*
  - Android..... 12
  - BlackBerry..... 12
  - iPhone..... 13
  - Windows Mobile..... 13
- Meeting Security Validations..... 13*
  - Android..... 14
  - BlackBerry..... 14
  - iPhone..... 14
  - Windows Mobile..... 14
- Allowing Security Extensions ..... 14*
  - Android..... 14
  - BlackBerry..... 15
  - iPhone..... 15
  - Windows Mobile..... 15
- Relative Strengths and Weaknesses of Each OS..... 15**
- Figure 1: Comparative Evaluation of Secure Mobile OS Components ..... 16*
- Conclusions..... 16**



## Choosing an Enterprise-Class Wireless Operating System: A Comparison of Android, BlackBerry, iPhone and Windows Mobile

### Introduction

Mobile deployments in business are growing at an accelerating rate, enabled by increasingly capable devices at attractive prices, faster, less costly, and more reliable wireless networks being deployed across wider areas, and an expanding array of mobile applications that empower the mobile workforce with an abundance of business critical functions. However, one of the critical hindrances to broader adoption, especially in those businesses with regulatory compliance or enhanced security requirements is the fear of data loss and/or data leakage. To prevent the potential loss of critical data and avoid the rapidly increasing cost of remediation that result from any data breaches, companies must assure the highest levels of security are fully addressed before implementing large scale deployments of mobile devices.

Security considerations remain the single biggest limitation to more aggressive expansion of wireless device usage in many enterprises. Regulated industries (e.g., financial, insurance, investments, retail, legal, health care, public sector) can not afford to deploy anything that could possibly compromise their data/records security or prevent meeting regulatory compliance requirements. Portable devices, easily lost and/or stolen, represent a threat that while real, can be managed with proper planning and foresight. The first step in making the mobile environment safe for both the end user and the corporation, is selecting a device that exhibits high levels of inherent security and manageability. To this end, not all devices are created equal. It is imperative that companies evaluate a potential device selection based on its intrinsic platform security capabilities, particularly around the security embedded within the device Operating System (OS).

In our whitepaper, “*Choosing an Enterprise Class Wireless Operating System (July 2008)*”, we discussed the ramifications of various selection criteria and the need to implement certain security policies and technologies. Further we discussed the market trends and the subsequent requirement for companies to choose wisely when selecting a mobile device. A review of the above whitepaper would be advantageous for the reader to understand the basis of the contents and analysis contained within this whitepaper.

This whitepaper will explore some of the key criteria necessary in selecting, deploying and managing a mobile operating system (OS) so that enterprise use of the device will not compromise the integrity of the company’s security efforts and put it at risk for costly legal and/or governmental actions. This whitepaper will compare the attributes of four mobile OSes, based on the guidelines presented in the previously mentioned whitepaper. The four operating systems are Android version 2.2 from Google, BlackBerry OS version 6 from Research in Motion, iPhone OS version 4 from Apple, and Windows Mobile OS version 6.5 from Microsoft (at the time of publication of this paper, Microsoft’s new Windows Phone 7 OS has not been released and is therefore not included due to incomplete details available for comparison purposes).



## Choosing an Enterprise-Class Wireless Operating System: A Comparison of Android, BlackBerry, iPhone and Windows Mobile

### Components of a Secure Mobile OS

There are a number of important components that make an OS secure and safe for business use. Below we identify some of the key attributes necessary to enable any secure mobile platform and which need to be evaluated by any organization considering the use of that platform. We then compare these attributes for the OSes being evaluated.

#### **Authentication**

Users should not be able to work on any device without adequate levels of authentication to prove he/she is the owner of the device. Passwords and two factor authentication (e.g., tokens, smart cards), are being deployed currently, with biometrics to be added in the near future, to insure that only the approved user of the device is allowed to access the functions and data on that device. Any device that can't be forced to require user authentication (through the setting of proper policies) should not be considered a security-ready, business-class device. Further, the ability of the end user to bypass and/or defeat authentication requirements should disqualify the device for any user accessing and maintaining corporate sensitive data, either in emails, or in accessing back office applications. Proper authentication is the first barrier of defense in any secure system, and should not be taken for granted.

#### ➤ **Android**

Android provides enforcement for a limited set of policies for user password/authentication through the use of ActiveSync which can only be controlled through a connection with Microsoft Exchange. It does not provide a way to effectively set and enforce complex authentication/password policy by an organization's IT department directly without using a third party product, or through a device manufacturer's additions to the core OS. Further it has no mechanism for adding two factor authentication capability. Finally, Android has no management mechanism that allows the device policies to be "locked" to prevent end user intervention and/or defeat of those policies.

#### ➤ **BlackBerry**

BlackBerry allows the company IT department, through use of the BlackBerry Enterprise Server (BES) tools, to set a robust policy mandating that the user must log in to the device via a strong password. Further, BlackBerry allows token-based two factor authentication and secure peripheral authentication devices to be added (e.g., card reader). Once the authentication policy has been set by IT, the user does not have the ability to bypass and/or reset this policy on his/her device. Further, IT can verify that required policies are in place and easily deploy them to devices through Over-The-Air (OTA) connections. A highly granular (e.g., by user, group, entire population) policy setting capability assures that different users can have unique policies specifically addressing their needs and/or job function.



## Choosing an Enterprise-Class Wireless Operating System: A Comparison of Android, BlackBerry, iPhone and Windows Mobile

### ➤ **iPhone**

The iPhone provides a log-in password that allows locking of the device and access/authentication of the user. The characteristics of the password (e.g., length, characters) can be set by the IT department by deploying a policy to the device. In earlier versions of the iPhone, the user had the ability to override IT policy configurations on the phone to defeat this function if he/she chooses. Current versions allow “locking” of the policy settings so users can’t alter them, but users can still delete them which will cause the phone to no longer function. Policies can be enforced by using ActiveSync through Exchange connectivity. The device supports token-based two factor authentication through use of SecureID or CryptoCard. All iPhones require connection to a PC running iTunes for initial activation on the carrier network. The iPhone, when connected to a desktop with iTunes installed, and when configured to sync automatically with iTunes, will create a complete backup of the device on that PC unless explicitly programmed not to do so. Therefore, the image, including all of the data on the device, could be accessible from a PC that the iPhone has been connected to, thus posing a potential security threat, although iTunes backups can now be encrypted through a policy setting. It is important to note that many of the log-in enforcement policies available for the iPhone require that the company run Exchange 2003 or 2007 with ActiveSync, which is used for such policies as password length, characters used, maximum number of failed attempts, device wipe, etc.

### ➤ **Windows Mobile**

Windows Mobile does provide for password locking of the device and does support a number of third party applications that create two-factor authentication (e.g., SecureID, card readers). Further, some Windows Mobile devices come with biometrics installed (e.g., finger print reader) and manufacturers of devices have the ability to extend the devices with a variety of authentication enhancement if they desire. Certain device functions can be managed and policies set via ActiveSync and Exchange so that users are required to authenticate in a strong manner, and once set through the IT department, users are not able to bypass these policies. However full policy setting capability requires the use of Microsoft System Center Mobile Device manager (MSCMDM) which is a unique product that requires purchase and is not integrated into other Microsoft products (e.g., Exchange, MSC).

### ***Data Vaulting***

The need to safely store data on the device, and any external storage, (e.g., SD cards), is a key requirement for any mobile worker with access to company information. Indeed, Data Vaulting offers a second level of protection in conjunction with authentication against device “hacking”. All levels of security for any data file and for every application on the device should be selectable by policies administered by the device and/or corporate security administrator as defined by company security policy. This should be enforceable at all times, and not just on some of the data some of the time. Some platforms require that all data on the device be either encrypted or not encrypted. However, certain forms of data on the device should be able to be selected to “unprotect” mode, for those files generally not



## Choosing an Enterprise-Class Wireless Operating System: A Comparison of Android, BlackBerry, iPhone and Windows Mobile

needing protection from prying eyes (e.g., MP3s, camera photos). Therefore, one criteria of any best-of-class device should be the ability to granularly select files and functions that need encryption, and those that do not, and have the platform act accordingly.

### ➤ **Android**

Android does not currently provide any hardware assisted encryption of data resident on the device, nor does it provide for external memory (e.g., SD cards) to be protected where data and/or applications may reside. Therefore, should someone get beyond the password (or remove the SD card), data will be exposed and accessible to that user. Further, password policy is managed through ActiveSync and can be altered by end user intervention, although such actions may prevent future connectivity to the Exchange server if such a policy is set on the Exchange server by IT. Third party and/or vendor extensions are required for companies that want to meet minimum security standards for protecting data and minimizing data leakage, but lack of any hardware assisted encryption is a significant handicap to Android's security capabilities.

### ➤ **BlackBerry**

BlackBerry provides a granular ability to encrypt all data on the device, including data stored on peripheral flash memory cards (e.g., SD cards). Further, policy setting flexibility allows the selective encryption of data, enabling full protection for company sensitive and personal data, but also providing for non-critical data (e.g., personal music files, images) to be stored unencrypted. This allows the device to use less processing power when retrieving the information and presenting it to the user, and ultimately can increase battery life and user performance. Data can also be selectively encrypted and protected on an application level to prevent unauthorized applications from accessing sensitive or confidential data. Finally, encryption can also be enabled in such a way that data is either locked to a user (via password) or locked to a user and device so moving the data to other devices is impossible.

### ➤ **iPhone**

The current iPhone does provide hardware assisted data encryption for all resident data on the device. It further allows for explicit protection of email messages and attachments, preventing this data from being accessed when the device is locked. A policy setting is also available that forces encryption of any device data backed up using iTunes. However, encryption for the device is not granular, and does not allow for selection of which files are stored encrypted and which are not.

### ➤ **Windows Mobile**

Windows Mobile provides the ability to encrypt peripheral data cards (SD cards), although the main memory of the device is not so encrypted. The inherent capability allows either full encryption or no encryption and does not allow granularly selecting which data to encrypt or leave unprotected. To enable this function automatically as a policy setting requires the use of MSCMDM and version 6 or greater of Windows Mobile (older devices are not encryption enabled). A manual setting is also available on the device, although most users would find it difficult to drill down through several menu levels to activate this feature. Any encrypted files



## Choosing an Enterprise-Class Wireless Operating System: A Comparison of Android, BlackBerry, iPhone and Windows Mobile

saved to a desktop with ActiveSync are stored on that PC in unencrypted format, and thus accessible by anyone using that PC. There are several third party applications available that do provide granular data protection and enhanced security protection, including for older devices.

### ***Application Verification***

To ensure maximum protection to both the platform and the data, devices should contain a mechanism for verifying that an application is indeed “who and what” it claims to be. Enterprise-class mobile platforms include a method for assessing signatures of various applications that, when checked by the device, can determine an authentic, non-tampered with application, from one that has been modified and/or contains suspect code. Clearly, the ability of the OS to distinguish between legitimate, safe applications and potentially destructive ones offers a major enhancement that any best-of-class mobile device should incorporate. This is an important defense against both malware and rogue applications that could cause havoc with the proper and effective use of the device. As a further requirement, IT must be able to control the approval of any applications resident on the device, and the user must be prevented from tampering with these controls.

#### ➤ **Android**

Android applications run in a virtual machine environment and do not have an explicit signature issuing authority (i.e., signatures may be implemented by the application creator without verification of the application or the creator). Applications may consequently be “spoofed” and/or malicious, and can cause problems within the device and potentially compromise both the device and its data. Android does run each application independently in its own virtual machine, which should help isolate problems between applications, but there is still the potential to falsify signatures and create malicious products. Android currently has no way for companies to set policies to enable/disable applications and/or device functions, unless enabled through vendor enhancements to the core OS.

#### ➤ **BlackBerry**

BlackBerry includes an inherent mechanism for verifying the signature of each installed application to assure the application has not been tampered with. Further, IT may set policies to allow or disallow individual applications from running on the device (e.g., turning off the camera or media player, preventing user installed application packages) and/or utilizing various resources and data already on the device. The application verification is available for company/IT use so that internally deployed applications can be signed and verified before being installed on the end users’ devices. Finally, once a policy is set the user does not have the ability to alter these policies or override them. BES provides the ability to do direct downloads and updates of any applications companies choose to run on the device either OTA or through “side loading” without requiring user intervention.

#### ➤ **iPhone**

All corporate applications require a digital certificate issued by Apple. To obtain the certificate the company must register with Apple. A Distribution Provisioning Profile must



## Choosing an Enterprise-Class Wireless Operating System: A Comparison of Android, BlackBerry, iPhone and Windows Mobile

then be created and must be loaded to each device through end user intervention (e.g., through clicking on an email attachment or through clicking on a link on a trusted website). Without this process, any application that has not been created by Apple will not function. This can prevent “rogue” applications from running on the device. However, “Jailbreak” programs are available on the Internet that bypass the iPhone security and allows unsigned applications to run on the device. If downloaded by the end user, this represents a significant threat to the security of the device. Loading corporate applications to the iPhone requires either uploading that application to a special area on Apple’s App Store for delivery OTA to each device, or by connecting each device to a PC and “side loading” the application through iTunes. This is true of any needed updates as well. There is currently no direct OTA mechanism for companies to transparently download applications to an iPhone. Apple recommends that enterprises install iTunes at each user’s PC to make application deployments and updates easier, which could present a security issue. This process requires users to initiate any downloads to the device from their PC or requires that IT retrieve each iPhone and “side load” through a master PC within IT control. Apple does provide an ability to disable some functions of the device (e.g., Web browser, media player, camera) through policy settings.

### ➤ **Windows Mobile**

Windows Mobile has limited ability to verify individual applications. It does allow the “signing” of executables and setting specific policies to limit which applications can run on a device. However, this requires that specific policies be set on each device through management intervention, and is not implemented by default on each device. This potentially enables a “rogue” application to be installed on the device. Much like Windows on PCs, Windows Mobile has a variety of mechanisms to deploy and operate applications. Windows Mobile does provide for OTA downloading of applications, and companies/IT departments can produce and deploy applications on their own without intervention. But as many Windows Mobile applications are quite large, side loading of the applications is often preferred to save time and limit telecom charges. Using MSCMDM, policies can be set on the device to enable or disable applications and to prevent the user from loading and/or changing or resetting the permission settings of various applications.

### **Reliability**

Any enterprise-class mobile OS should exhibit the reliability end users expect from a robust mission-critical device. This means that the device should never simply decide not to work (e.g., “Blue Screen”), or require unexpected re-boots. Further, in a working-class device, any peculiarities with the OS (e.g., crashes, freezing) will likely cause more than just inconvenience – they will cause work to be lost, lowering overall productivity and raising support costs, not to mention increasing end user frustration levels. This may be acceptable in a consumer device, but not in an enterprise-class production device. Companies should make sure that any mobile OS being evaluated for its mobile workforce be examined for its reliability and capability to withstand the rigors of the mobile work model.



## Choosing an Enterprise-Class Wireless Operating System: A Comparison of Android, BlackBerry, iPhone and Windows Mobile

### ➤ **Android**

Android may be implemented differently on each manufacturer's device and therefore there is some variability in the robustness of the products. Further, due to the more open nature of Android, it is possible that badly formed applications can cause operational problems with the device. Vendor's must therefore design in and test for enterprise-class reliability enabled by their particular implementation. Users may experience stability and reliability variations among different Android-powered devices depending on manufacturer and OS Version.

### ➤ **BlackBerry**

BlackBerry devices have generally exhibited a high degree of stability and a lack of freezes and crashes. As a result, few users have reported problems with work being lost due to device problems and devices rarely require a re-boot.

### ➤ **iPhone**

The iPhone has very few unexpected OS interruptions and works very well for most users. There have been few reports of freezing or crashes and users report high levels of productivity when using the device.

### ➤ **Windows Mobile**

Windows Mobile has, much like its PC OS cousin, been known for OS crashes and freezes. Although newer versions of the OS have been improved, users still report application crashes which are annoying and can cause the loss of work and data. Most crashes require a re-boot of the device.

## ***Manageability and Policy Enforcement***

A device that can't be remotely managed will add significant amounts of TCO and additional support burdens to any organization deploying it. Companies evaluating devices should examine whether the device OS offers hooks to manage all aspects of the platform (e.g., set up, monitoring, uploading, display of device characteristics, asset management, lock down and kill, re-imaging to a new device, OS software upgrades). If such capability is not inherently available within the OS, it is highly unlikely any security and/or management tools will be able to competently manage all of the functions necessary in a complex, current generation smart phone. Further, companies should examine whether policies can be set up for individual users on specific devices, whether policies can be created to take into account various user classes and/or device characteristics, and whether different apps and different data can be provisioned for different classes of users on a case by case basis. All of these functions should be available within any platform designated for efficient and productive organizational use.



## Choosing an Enterprise-Class Wireless Operating System: A Comparison of Android, BlackBerry, iPhone and Windows Mobile

### ➤ **Android**

Android has very limited remote management capability natively that can be accessed by IT staff. It does provide for some management through ActiveSync policy settings or through third party tools. But more robust device management requires vendor enhancements or a specialized third party application, but even here the amount of management is comparatively limited. In future, Android will likely develop management APIs that can help with this process, and we expect some vendors to add this capability to their devices as a value-added solution.

### ➤ **BlackBerry**

BlackBerry has been designed to be managed by a set of policies that can be easily created and granularly deployed through the standard BES required by all BlackBerry installations. Policies are delivered OTA directly to the device and configured automatically without user knowledge or intervention required. Currently, there are over 400 individual policies that can be set. Further, once policies have been set, they can be completely enforced with no possibility of the user bypassing the settings. Data logs of each device are available for analysis. Additionally, various “hygienic” readings of the device can be taken to indicate its memory use, battery condition, overall health, etc. This can be very useful in determining potential problem conditions of the device, as well as understanding the users’ needs and future application/policy modifications.

### ➤ **iPhone**

iPhone provides the ability to manage devices through a policy setting function through its iPhone Configuration Utility. Once policies are set and installed on the device, they can only be updated through the resending of a new policy file. This can be accomplished through a side-loading capability from the configuration utility running on a PC or Mac. Configuration files can be encrypted and assigned to individual devices to prevent tampering. iPhone has recently added the ability to deliver encrypted configuration files over the air using a Secure Enrollment and Configuration Process (SECP), but requires creation of custom configuration profile files by the organization. Alternatively, this can be accomplished via an email with attachment or through browsing to a web page and downloading a link. In either case, this requires a manual process and the update process is not transparent to the end user. IT does not have total control and should the user choose not to update, there is no way to “push” the updates to the device and enforce their application. Further, there is no current way to monitor the settings and “hygiene” of individual devices or to easily retrieve log files from the device to assess usage and/or user patterns.

### ➤ **Windows Mobile**

Windows Mobile does allow various policies to be set and managed through the MSCMDM functionality, provided the device is at least version 6 of Windows Mobile. Further it does make some log files and other hygienic data available to the IT administrator. There are a number of third party management applications available that provide more extensive management and information retrieval of Windows Mobile devices than Microsoft currently provides.



## Choosing an Enterprise-Class Wireless Operating System: A Comparison of Android, BlackBerry, iPhone and Windows Mobile

### ***Tamper Resistance***

Companies should always seek to discover whether any device has been “hacked” or attempts have been made to alter the base level OS. While Malware is not yet a major problem for smart phones, it will be in the near future as more “hackers” view the increasing number of smart phones as an attractive target. The more tamper resistant the OS, the less likely that malware can infect and compromise the platform, reducing risks for the company in both safekeeping the individual device and its data, but also in stemming any spread of the malware. An OS that only allows applications to run at a higher level than the core of the OS (e.g., in a Virtual Machine) represent a much lower security risk to the organization than one that allows applications to get deeply into the core of the OS. Companies should at the minimum evaluate the platform’s ability to make the administrator aware of any problems, and preferably provide a sanitized area to contain applications to prevent infections.

#### ➤ **Android**

Programs in Android run in a “sandboxed” virtual machine environment, providing a layer of protection. Applications can request resources and data from other components, but approval is required for access. Android explicitly allows programmers to write “device administrator” programs that can control security parameters of the device. While useful for management functions, this capability can potentially be used by rogue programs to compromise the device. Android’s open programming model is not adept at preventing hackers or rogue applications from compromising the security of the device and its data. And the extensibility of Android allows various vendors to modify the underlying system, potentially exposing new tamper points. We expect that vendors and/or third party solutions will add enhancements to the core OS improving its tamper resistance.

#### ➤ **BlackBerry**

BlackBerry is very difficult to hack, as the OS must boot in a known state with a known signature before the device will initiate. This means that the OS itself is checked before each boot. Further, since third party applications run in a Java Virtual Machine, hacking into the base operating system of the device is extremely difficult if not impossible. This makes it very difficult for malware and rogue applications to affect the core operations of the device. Finally, policies can be set for specific applications or types of applications that guard against their infiltration into protected areas of the device and/or its data.

#### ➤ **iPhone**

The iPhone OS is difficult to access on the device as Apple has limited the methods for accessing its core functions and has “sandboxed” running applications. However there have been a number of successful attacks against the Safari browser that has left the device compromised. Applications run in administrator mode, so once an application has gained access to the device, it can interact with virtually all of the functions and data available on the device. Since the iPhone OS is based on the same core code as the Apple Macintosh Mac OS X, and there have been indications that malware is now emerging for the Macs, it is



## Choosing an Enterprise-Class Wireless Operating System: A Comparison of Android, BlackBerry, iPhone and Windows Mobile

likely we will see increasing amounts of malware for the iPhone as well. Further, there have been examples of applications that were able to get around many of the protections of the OS by accessing supposedly inaccessible applications and retrieving data (e.g., contact information). This indicates that the OS still has some maturing to do to be fully robust and secure. Companies must be cautious as we expect to see malware attacks in the near term due to the popularity of the device.

### ➤ **Windows Mobile**

Windows Mobile has exhibited hacking friendliness in the past, as many of its core functions are exposed through its APIs and the amount of detection and prevention of tampering and rogue applications it can perform is limited. There are currently a growing number of third party applications for anti-virus and malware prevention, much as in the PC world, and we expect to see malware attacks become more common in the next few years.

### ***Security vs. Usability***

Nearly any mobile OS can be secured by totally locking down the device and preventing any meaningful interactions with the OS. However, while it certainly is important to maintain the highest level of security possible, this must be done while maintaining the usability of the apps and end user interface. Creating an environment that enables maximum usability while maintaining the integrity of the system requires a delicate balance. Companies looking for highly secure devices should evaluate the level of security in conjunction with the usability of the system, and whether or not the end user finds the OS easy to use, navigate and customize for reasonable personal preference needs. One size does not fit all, and the level of security must be balanced against the needs of the user community. However, the final choice should be weighted more heavily towards security than usability if a tradeoff must be made.

### ➤ **Android**

Android has very little capability of locking down a device, other than implementation of a limited number of policies enabled through ActiveSync. Android weighs in heavily on end user control, with very limited organizational control capability provided. Further, many vendors add a layer of user interface on top of the core Android OS to enhance the functionality. Organizations should evaluate these vendor usability enhancements and determine whether they add to or detract from the overall security of the device.

### ➤ **BlackBerry**

BlackBerry provides an extensive number of policies IT can manage on the device, all from within the control of the BES administration function. All policies can be delivered to the device through OTA deployment. IT has complete control over which policies are set and the end user can not override or access the forbidden functions once set up through the BES. This assures that IT is in complete control. It also allows the BES to act as a single control point for all features, functions and policies for all devices in use. Further, this mode of security makes it transparent to the end user, as it is fully integrated within the OS and



## Choosing an Enterprise-Class Wireless Operating System: A Comparison of Android, BlackBerry, iPhone and Windows Mobile

requires no knowledge or intervention on the part of the user. Finally, individuals or groups of users can have customized policies to provide the maximum balance of protection versus usability depending on functions and/or job classifications.

### ➤ **iPhone**

While the iPhone does provide some capability for managing the device and setting policies via the iPhone Configuration Utility, and Configuration Profiles, the number and type of policies that can be set is limited. Further, the profiles have to be explicitly delivered to the iPhone OTA and accepted by the user, or alternatively either via users surfing to a secure web page and installing the profile, or through delivery of the profiles in an email message which users then install by tapping on the attachment. This “user intervention” puts the burden on the user to initiate the profile installation before any policies can be set by the IT department. This is a very insecure way of configuring a device, and the company has no way to force compliance and/or monitor whether all of the profiles have been set.

### ➤ **Windows Mobile**

Windows Mobile devices can be managed through deployment of MSCMDM. This product extends many management functions available within Exchange to the device and is the primary way for the device to be enabled with VPN, device encryption, and the device wipe functions included within ActiveSync. However, MSCMDM is not currently integrated into existing system management tools (e.g., MMC) used to manage desktops and servers and as such requires a stand alone implementation. Further, it requires the addition of at least one and possibly several stand alone servers to deliver its functionality. And although it is transparent to the end user once installed and running, the initialization and set up does require some end user intervention on the device. While improved from previous versions of the Windows Mobile OS, there are still some areas that need to be enhanced to meet broader company and user requirements.

## ***Meeting Security Validations***

Many industries require that devices be validated and approved by governmental agencies to ensure that they meet stringent security testing and specifications before they can be deployed to mobile workers. While a number of devices claim to be “compatible” with security standards like FIPS-140-2 encryption, it is imperative that they have been tested and approved by a validated testing agency and not just offer claims of compatibility. Further, new security standards are evolving and will be required for certain classes of users. The ability to prove compatibility with these emerging standards is imperative in many industries and government agencies. Although an entire platform is tested, no device can meet the challenge of security validations without having an OS that is capable of meeting the stringent approval process. Therefore, companies looking for a device with maximum security should begin by looking at the OS and whether it is capable of being validated against a variety of security standards, and preferably choose one that has already undergone verification testing and has been accredited.



## Choosing an Enterprise-Class Wireless Operating System: A Comparison of Android, BlackBerry, iPhone and Windows Mobile

### ➤ **Android**

Android has not met any security validations, nor has Google indicated it intends to do so in the foreseeable future. And with a lack of hardware encryption capability, it is not capable of meeting any of the common security validations. We expect some vendors to add enhancements that allow them to move towards validation as a way to make their devices more attractive to corporate deployment. But currently Android is unsuitable for organizations requiring certification of their devices.

### ➤ **BlackBerry**

BlackBerry has applied for and attained numerous validations/certifications for its devices, including FIPS 140-2, NATO Restricted classification, UK CAPS Restricted classification, and Common Criteria EAL 2+ certification. BlackBerry does include the ability to select the most common encryption algorithms (e.g., AES, 3DES) to protect the data on the device, and provides a complete remote device wipe capability as well. BlackBerry provides the most secure mobile OS available on the market.

### ➤ **iPhone**

Apple has not declared any intention to seek regulatory certification/validation of the iPhone. Further, normally expected security features like remote device wipe for the iPhone require that ActiveSync and Exchange 2003 or 2007 be deployed at the company. Although it does have on board hardware assisted AES encryption capability, it is unlikely the iPhone will meet any of the security validation requirements in the near term.

### ➤ **Windows Mobile**

Windows Mobile 6 devices do provide encryption capability for a variety of common standards (e.g., 3DES, AES) and do provide for remote device wipe through the ActiveSync capabilities when used with MSCMDM and Exchange. However, although Microsoft is pursuing validation for its devices for FIPS, it has not yet been more broadly recognized by other validation bodies. Several third party vendors do provide solutions that upgrade the products to meet some of the validation requirements

## ***Allowing Security Extensions***

No one vendor can provide everything necessary for all circumstances now and in the future. Companies may have a security need not currently available as an integral part of the platform. An ability to extend the security model should be provided by the vendor through an API. This allows extensions as required (e.g., S/MIME, PGP, RSA). Companies that must implement specialized security enhancements should evaluate the platform for its ability to be extended and conform to those needs in a safe and flexible manner.

### ➤ **Android**

The open nature of Android allows for many add-on capabilities not native to the core OS. This allows device vendor extensions and third party security solutions. However, as each



## Choosing an Enterprise-Class Wireless Operating System: A Comparison of Android, BlackBerry, iPhone and Windows Mobile

vendor implements its own version of what it believes is needed, there evolves a lack of commonality across the different solutions. Further, third party secured applications do not generally run within the native Android applications. Nevertheless, organizations with security concerns should evaluate each device's extended security characteristics when available from the device vendor or a third party provider.

### ➤ **BlackBerry**

BlackBerry, through its APIs and special third party programs, provides a mechanism for extending the security of its devices, both with third party application providers as well as with business customers.

### ➤ **iPhone**

iPhone does not provide a specific mechanism for extending the security on the device, other than enabling applications to use some of the installed security features (e.g., hardware encryption). While it does provide limited SDKs and APIs for the device, these are geared towards application developers and do not provide the low level OS calls needed to extend the existing security model. Indeed, most third party security enhancements to the iPhone exist as unique applications running on the device, and the user is therefore not within the native device application. The implication of this is that each application must create and enforce its own security, rather than having a blanket security application that runs across all applications installed on the device

### ➤ **Windows Mobile**

Windows Mobile's design philosophy is very similar to Windows and does provide APIs that allow extensions of many aspects of the underlying OS as well as the native apps. It is relatively easy therefore to build security enhancements that work across all of the device functions and native applications. Further, this approach has also been used to provide anti-virus and malware capability for the device.

## Relative Strengths and Weaknesses of Each OS

Figure 1 below represents our comparative analysis of the four operating systems. This is a subjective evaluation based on our assessment of the strengths and weaknesses of each. It is intended to provide a guide to which products are acceptable and which have shortcomings in the key areas identified in this whitepaper. It is understood that the OSes will change and evolve over time, but our assessment is based on the current version of the products at the time of this writing.



## Choosing an Enterprise-Class Wireless Operating System: A Comparison of Android, BlackBerry, iPhone and Windows Mobile

**Figure 1: Comparative Evaluation of Secure Mobile OS Components**

	BlackBerry OS	iPhone OS	Win Mobile OS	Android OS
Authentication	↑↑↑	↑↑	↑↑	↑
Data Vaulting	↑↑↑	↓	↑↑	↓↓↓
Application Verification	↑↑	↑	↑	↓
Reliability	↑↑↑	↑↑↑	↑↑	↑↑↑
Manageability/ Policy Enforcement	↑↑↑	↑↑	↑↑	↑
Tamper Resistance	↑↑	↑	↑	↑
Security vs. Usability	↑↑	↓	↑↑	↓↓↓
Meeting Security Validations	↑↑↑	↓↓↓	↑	↓↓↓
Allowing Security Extensions	↑↑	↑	↑↑	↑↑

Copyright 2010 J.Gold Associates, LLC.

### Conclusions

Wireless mobile devices represent a potential security challenge for organizations with a highly mobile workforce. However, the amount of risk can be managed by carefully selecting an enterprise-class platform with an OS that has included the important features needed to secure the device and data contained therein. We have provided a comparative analysis of four mobile platforms, including an indication of the strengths and weaknesses of each.

Our analysis shows that while each may have strengths and shortcomings, the most secure platform for business use is the BlackBerry platform. Windows Mobile has continued to



## **Choosing an Enterprise-Class Wireless Operating System: A Comparison of Android, BlackBerry, iPhone and Windows Mobile**

improve over its years in the market, and has implemented some significant security enhancements to its recent version, but is still not of the caliber of BlackBerry. It may be a viable option for companies that are able to circumvent its shortcomings through third party add-ons. However Microsoft is about to release a completely new mobile OS and the long term prospects for Windows Mobile are unsure. The iPhone platform has advanced towards being enterprise-class but still has some shortcomings when it comes to business-class security, and is not recommended for businesses that are concerned about maximum protection for data that might be contained on the device, or for any company that might be subject to rigorous compliance issues. The Android platform is the least secure of the four we evaluated, a reflection of its immaturity and lack of enterprise focus. Some Android device vendors are extending the base platform to be more enterprise friendly and future devices, especially as a result of these extensions, should improve. Companies choosing Android devices should only acquire them from vendors that have enhanced their manageability and security features.

Companies should remain vigilant and balance their user wants and needs for a device with the necessary requirements to protect company confidential information through deployment of “designed for security” platforms and their corresponding enabling technologies behind the company firewall. Companies failing to make wise choices and secure their mobile devices will face major problems resulting in fines, regulatory non-compliance, potential legal challenges and ultimately loss of revenues.



### **About J.Gold Associates**

Founded by an internationally recognized expert and industry veteran with over 35 years of experience in engineering, product marketing, market research and analysis, and technology advisory services, J.Gold Associates provides its clients with insightful, meaningful and actionable analysis of trends and opportunities in the computer and technology industries. We offer a broad based knowledge of the technology landscape, and bring that expertise to bear in our work. J.Gold Associates provides strategic consulting, syndicated research and advisory services, and in-context analysis to help its clients make important technology choices and to enable improved product deployment decisions and go to market strategies.



**J.Gold Associates, LLC**  
6 Valentine Road  
Northborough, MA 01532 USA  
+1 508 393 5294  
[www.jgoldassociates.com](http://www.jgoldassociates.com)