Enterprise Readiness of Consumer Mobile Platforms

Contents

Executive Summary

An increasing number of companies are opening corporate networks and data to consumer mobile technology. The resulting trend, usually referred as the consumerization of enterprise mobility, assumes even more disruptive connotations when the employees are allowed to use their own smartphones and tablets to work—commonly referred as BYOD or Bring Your Own Device.

Consumer technology is convenient, easy to learn, and fun to use. However, consumer technology is generally not as secure and manageable as required by the enterprise. Consumer technology brings real business value in terms of productivity and business agility. However, the lack of a strategic approach to the consumerization of IT creates security risks, financial exposure, and a management nightmare. Rather than resist it, organizations should embrace consumerization to unlock its business potential. This requires a strategic approach, flexible policies, and appropriate security and management tools.

A strategic approach to consumerization starts with a clear understanding of the security and management capabilities of each mobile platform. While no mobile platform is immune from security vulnerabilities and management limitations, some platforms are more mature than others with regard to supporting the most appropriate set of policies required by the different mobile roles within the organization.

This independent study offers an impartial and objective evaluation of today's four leading mobile operating systems: BlackBerry OS, Apple iOS, Windows Phone, and Android. In addition, it offers a comprehensive framework of analysis including 60 security and management criteria organized in 12 categories and a corollary guide for defining mobile roles and postures. This document is not intended to forecast adoption or market fate of individual platforms, because these are irrelevant to the IT managers who will likely have to consider some level of support for all of them anyway. Instead, the analytical framework and the experts' ratings are intended to provide a valuable tool for the definition of sound mobile policies. This allows IT managers to embrace consumerization with confidence and to turn it into a competitive advantage for their organizations.

Mobile Roles and Postures

The role-based methodology—by which a device's management and data protection are dictated by the role of its user or owner—is a trend taking place in many organizations that are thinking of new ways to profile the risk of mobile devices and their users.

Mobile device management tools have centered, to date, on device remediation. In many cases, the ability to lock or wipe a lost device, while important, does not do much to protect the data on the device or restrict the way in which the device can be used in terms of capture, storage, and transmission of information.

Roles such as general knowledge worker, contractors, occasional users, and, to a certain extent, managers are often exempt from the most stringent controls which require complex device authentication and encryption. That said, there are managerial roles that require ready access to highly sensitive information such as compensation/salary, details which, when stored on the mobile device of a manager, requires a more stringent set of controls. In the case of the contractor or occasional user, device risk profile may be heightened due to the sharing of devices among multiple, occasional users or the introduction to a personal or other organization's owned device in the case of a contractor.

Role	Description
Key Executive	Due to the high visibility of this user, they are susceptible to targeted attacks and planned device compromise. Of highest value may be email and contact data stored on the device for the launch of further spear-phishing attacks and blackmail efforts.
Manager	Handling employee personnel data and substantial amounts of product Intellectual Property, managers should be viewed in a similar light to compliance-centric workers.
Compliance-subject Worker	Working in operations areas such as HR and Finance, these users are regularly in possession of data subject to security controls dictated and enforced by various compliance requirements.
General Knowledge Worker	Due to the nature of their work, general knowledge workers like to have access to basic PIM functionality on their devices.
Field Worker	Similar to general knowledge workers, field employees may store data on devices when they are out of cellular network range. These users may require additional security controls as a result.
Contractor/ Occasional User	Contractors and other trusted non-employees have access to company data but are not subject to the same controls and policies due to their third-party status. While requiring data to perform their jobs, these users present a management challenge.

Table 1 – Mobile Roles Definition

It is also possible for a user to be a member of multiple groups. For example, many key executives also function in a manager role and many managers—or even general knowledge workers, because of their industry—may be compliance-subject, in the cases of multiple group membership, an employee's device security posture should default to the most stringent level of controls.

The table below is intended to serve as a catalyst toward—and not a substitute for—policy generation. Detailed profiles of the various user groups inside of any organization will likely bear resemblance to many of the groups outlined here but also differ in many ways and require more granular, less binary policy decisions. The granularity in decisions around device policy should also be driven by any relevant compliance standards that are likely to be far more prescriptive (with associated penalties for lack of compliance to the letter of the specification) in their demands.

Role	Device Encryption	Multi-factor Authentication	Local Storage Access	Data Filtering (DLP)	Complex Passwords	Attachment Access	Non-cellular Radio Use	Connection Encryption
Key Executive	■	■	○	●	■	■	■	■
Manager	■	●	■	■	●	■	○	■
Compliance-subject Worker	■	■	○	■	■	○	○	■
General Knowledge Worker	●	○	○	○	○	○	○	■
Field Worker	■	○	■	●	○	■	■	■
Contactor/ Occasional User	●	■	○	●	■	○	○	●

Policy Coverage	
Required	■
Nice-to-have	●
Not Required	○

Table 2 – Mobile Roles and Postures

Mobile Platforms Ratings

The analysis of the mobile security experts reveals that today's mobile platforms widely differ in terms of security and manageability capabilities. As a group, modern mobile platforms provide substantially better security than traditional desktop operating systems when it comes to built-in security mechanisms, authentication, and data protection; even though they are vulnerable to attacks that don't affect desktop PCs. Application security, device management, and corporate email support are somehow sufficient although they still have room for improvement. The feature sets that IT managers should give high consideration to include: security certifications, device firewall, and support for virtualization, which are largely still missing.

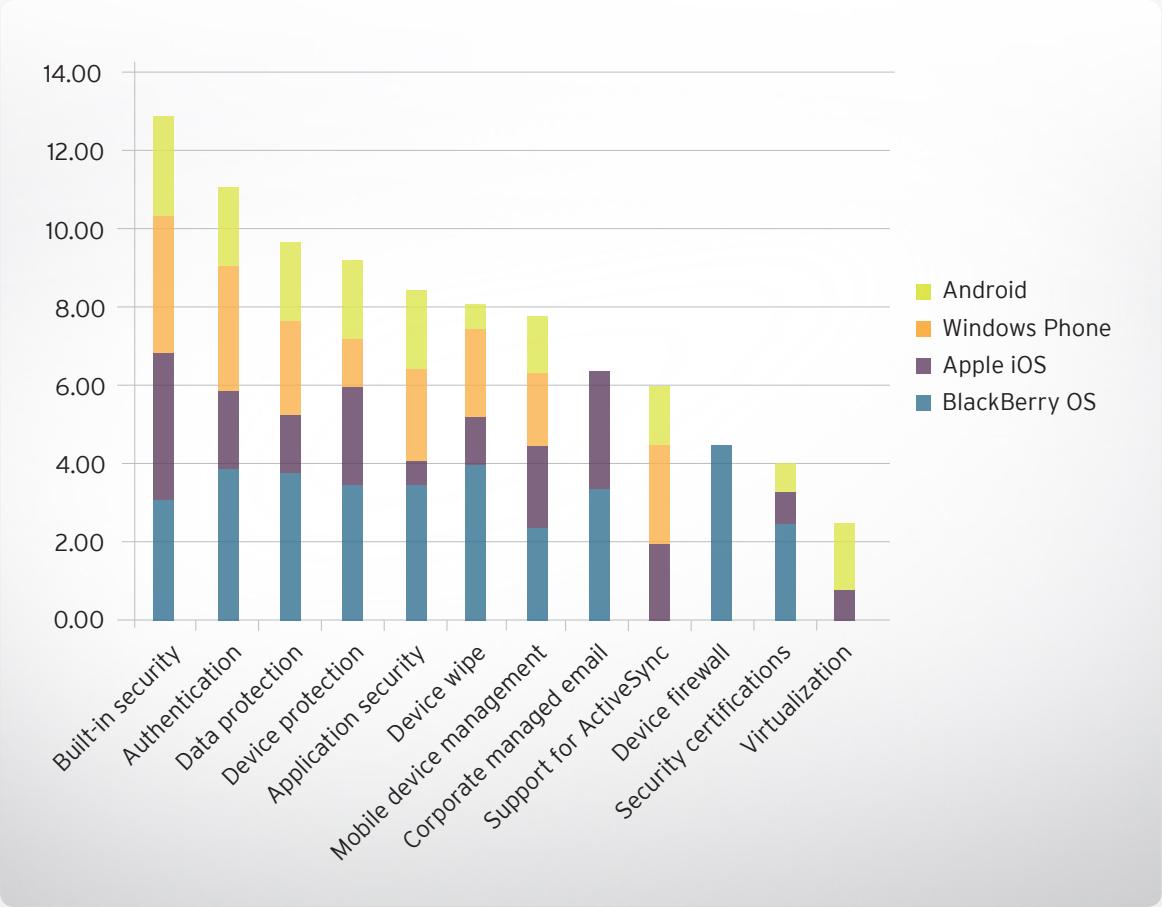

Figure 1 – Ratings by Category

BLACKBERRY OS. When it comes to individual platforms, the experts' analysis clearly points out that some operating systems are more mature than others. BlackBerry OS scores very highly across the board, clearly separated from the group of the three emerging consumer mobile platforms. Corporate-grade security and manageability make this platform the option of choice for the most stringent mobile roles.

APPLE iOS. Now at its fifth iteration, the leading challenger is Apple iOS. Apple's proprietary approach has become more enterprise-friendly: the strict control exerted by Apple on the overall ecosystem—from hardware to operating system to applications—makes this platform more secure and manageable in the consumer mobile segment. However, in contrast to RIM's fully integrated approach, the back-end components required to secure and manage Apple mobile devices are not provided directly by Apple but by a multitude of third-party vendors usually positioned in the Mobile Device Management segment. When complemented by third-party infrastructure, Apple iOS security and manageability are already good enough to be considered for mobility roles requiring device encryption and policy control.

ANDROID. Despite its impressive market performance, Android security and manageability are the lowest in the segment. The Google Android operating system is at its fourth commercial iteration and has recently seen some important security additions, such as device encryption support, however good Mobile Device Management APIs and a reliable control of the overall operating system versioning and application ecosystem are still conspicuous by their absence. The system is widely exposed to malware and data loss, and the platform fragmentation resulting from the rich OEM ecosystem has proved quite challenging for enterprise adoption. IT managers should definitely consider adding Android to their set of flexible policies but should probably limit its use to the least sensitive mobile roles.

WINDOWS PHONE. Although last to enter this segment, Microsoft Windows Phone performs quite well across the board especially considering that version 7.5 has only been out for less than 18 months. The system is too new to show a reasonable track record for enterprise adoption, and corporate policies should take this reality into consideration when considering Windows Phone devices for mobile roles other than for general knowledge workers.

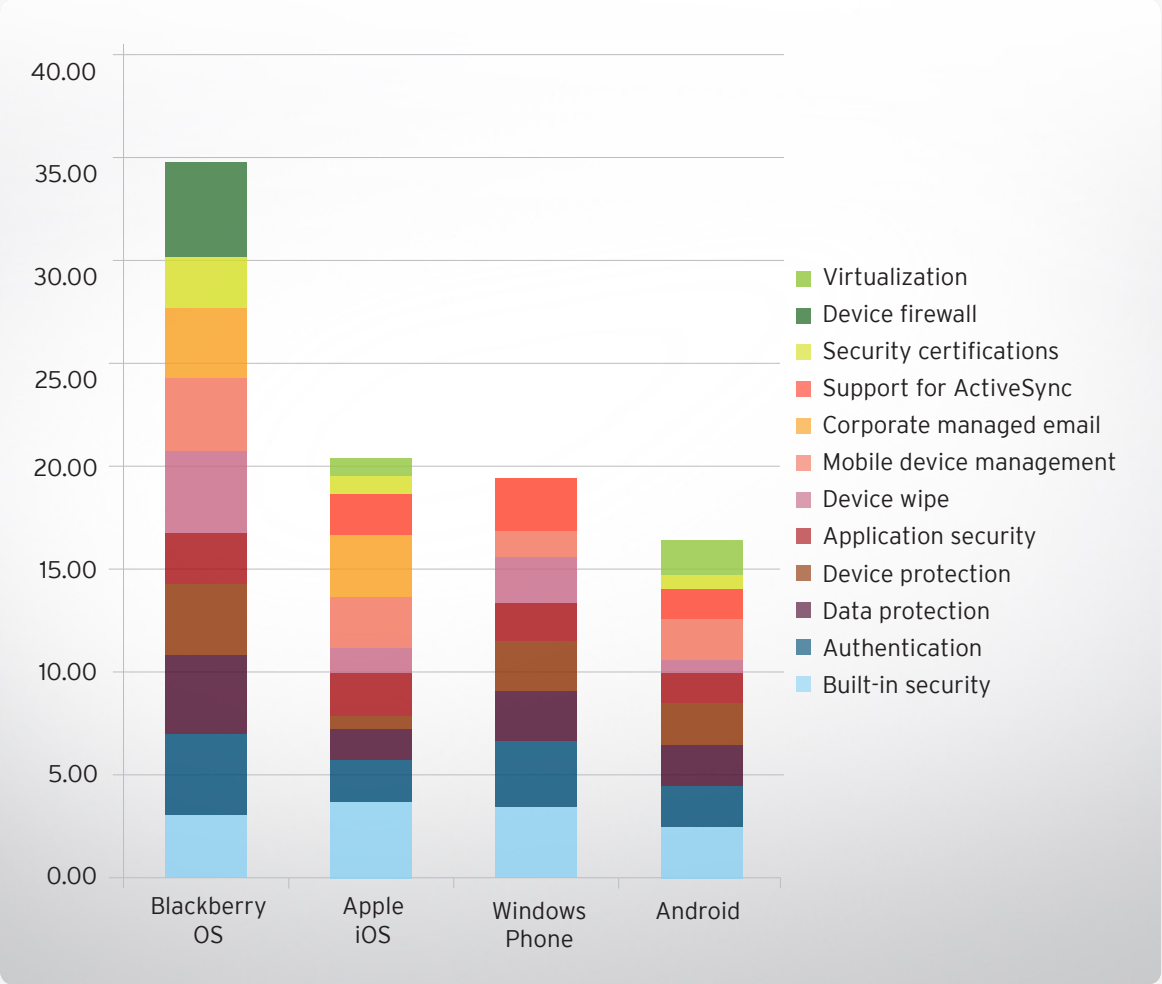

Figure 2 – Ratings by Mobile Platform

BlackBerry OS

With the advent of Research In Motion's BlackBerry OS 7.0 the Canadian smartphone maker's devices get a facelift and a handful of novel features such as touchscreens and Near Field Communication (NFC.) All of these additions are in hopes of resuscitating the handset maker's products among users who are increasingly providing and, in some cases, provisioning their own devices. BlackBerry devices, along with their back-end management through the BlackBerry Enterprise Server (BES) have been viewed by many as the bellwether for device security, with many endorsements and approvals of past versions of the OS bearing out that reputation. Many of the recent features added to the BlackBerry smartphone, and its associated OS, have been aimed at growing consumer appeal as it illustrates a large portion of RIM's customer growth both in North America and beyond. A new OS is expected later this year, though it is unknown whether the features set of the upcoming BlackBerry 10 will center more on consumer or enterprise-centric features.

Many of the features of the BlackBerry 7 OS are updates on existing capabilities we have seen in previous iterations of the OS. This is good in that RIM is building on a solid foundation for security, however, given the change in OS versioning, it requires a resubmission and testing for features like Federal Information Protection Standards (FIPS) 140-2 classification, which had not been completed at the time of analysis but has since been completed.

The strength in BlackBerry lies in the granular control—via IT policies—that are present on the BES itself. Devices associated with a corporate BES score quite well across security characteristics but it is critical to note than many features and protections that are commonly enabled or enforceable via the BES are not present on devices that are user provisioned via the BlackBerry Internet Services (BIS), which is a means for users to sync email, contacts, and calendars with Active Sync-enabled servers or personal, POP and IMAP mail servers. In fact, some of the strongest features, which restrict high risk activities that users may undertake, such as removal of password protection for the device, obfuscation of device encryption, and standard levels of complexity for device passwords may be rendered inactive if a user's devices is not provisioned via the BES. For this reason, in scoring the BlackBerry OS, many categories were shown to score in middling territory as their true use and enforcement relies on a complex, back-end infrastructure that not all organizations may have in place or want to maintain.

Research In Motion is at a turning point, both as a company and from a product standpoint. New leadership has re-confirmed that new devices based on the firm's upcoming BlackBerry 10 platform—a complete redesign of the device software—should be expected in the latter half of 2012. Along with this, the future of the devices' connectivity is expected as well, and it is not yet known for sure how BlackBerry devices will be managed in the next iteration of server and device software. BlackBerry 7 OS is likely the last version of "legacy" device OS we'll see coming out of Waterloo.It's a known quantity for enterprise device managers, though likely one that will be short-lived as new, BlackBerry 10-based devices are pushed into the market later this year.

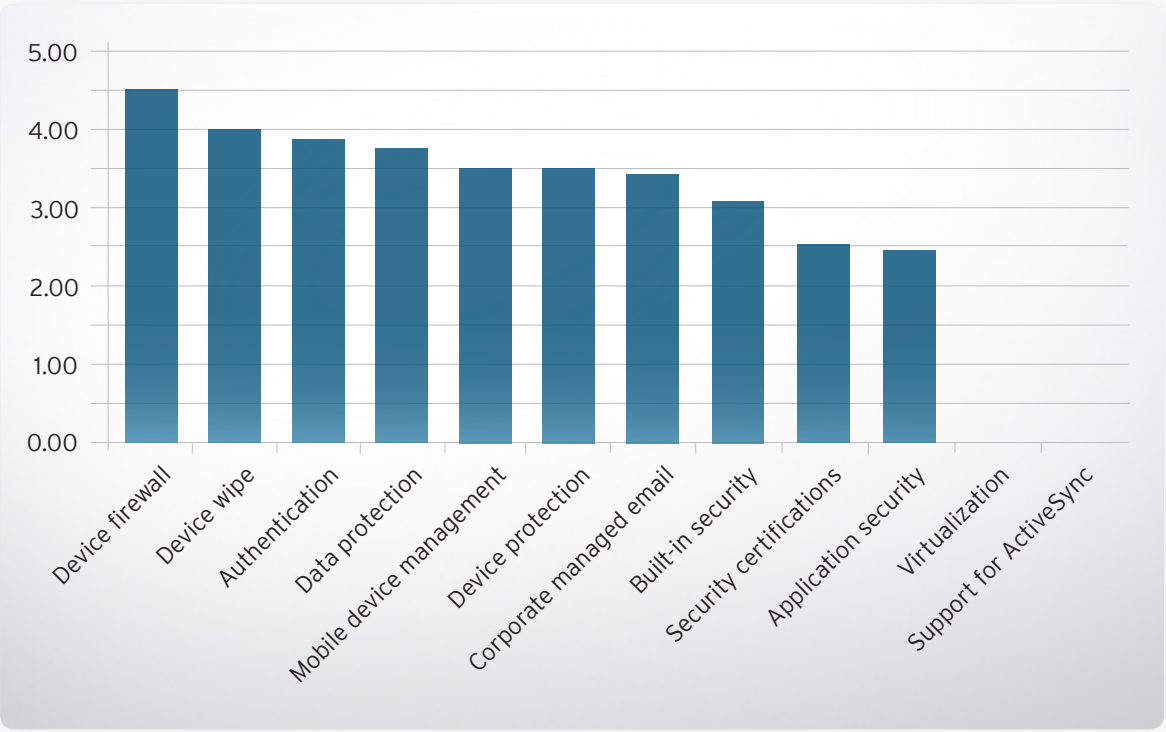

Figure 3 – BlackBerry OS Ratings

Apple iOS

With the wild success Apple has had with the iOS platform—both for the iPhone and the iPad—most individuals would incorrectly attribute the success to either first-mover advantage or the wildly successful App Store that has over 500,000 applications in its catalogue. This is not the true reason why Apple has been so successful with the iOS platform. The true reason for the success can be attributed to an incredibly focused vision on one thing: the user experience.

Even here though, people will think of the user experience in terms of the physical attributes of the hardware (which cannot be underestimated) or the fluidity of the operating system's user interface. While these two factors are certainly important, the user experience, as far as Apple is concerned, goes well beyond the "obvious" factors.

User experience for Apple also includes the quality of the applications that are provided to users in the App Store. Right or wrong, Apple has very strict guidelines for the approval process of the applications that third parties develop. This goes beyond user interface guidelines, but also to application performance management and in that, they include security. The iOS application architecture natively provides users much protection in terms of the fact that all applications are "sandboxed" in a common memory environment. The downside of this architecture is that theoretically you are only as strong as your weakest app. Security in iOS also extends to the physical attributes of the iPhone and iPad. There are no options for adding removable storage, which in effect provides another layer of protection for users.

Security within the iOS construct takes on other levels, specifically where no application can be installed or updated without the express consent of the user. Even if a company uses a mobile application management solution to "push" applications to an employee, the user still has to approve the installation request for the application to be on the device. Why? Because iOS is a user-centric mobile operating system.

One historical complaint of the iOS platform was that it did not have the same levels of security as the BlackBerry operating system. That was a very fair comment given that when iOS first came out, it had zero IT management policies, versus BlackBerry's 500+ (at the time). Today, iOS provides third-party mobility management ISVs for a number of native APIs that provide very competent "device management" capabilities (albeit nowhere near the 700+ that BlackBerry has). Again however, there is a difference in terms of the fact that with the BlackBerry platform, the IT administrator has complete control over the device, whereas in an iOS world, the IT department can configure certain things, but only once the user has provided certain permissions to the IT administrator.

Apple has radically changed the world's views on mobile security, moving it from a world where all policies were dictated by the IT department (regardless of how that impacted the actual users) to a model where the IT department has to now balance the needs of both the workplace and the workforce.

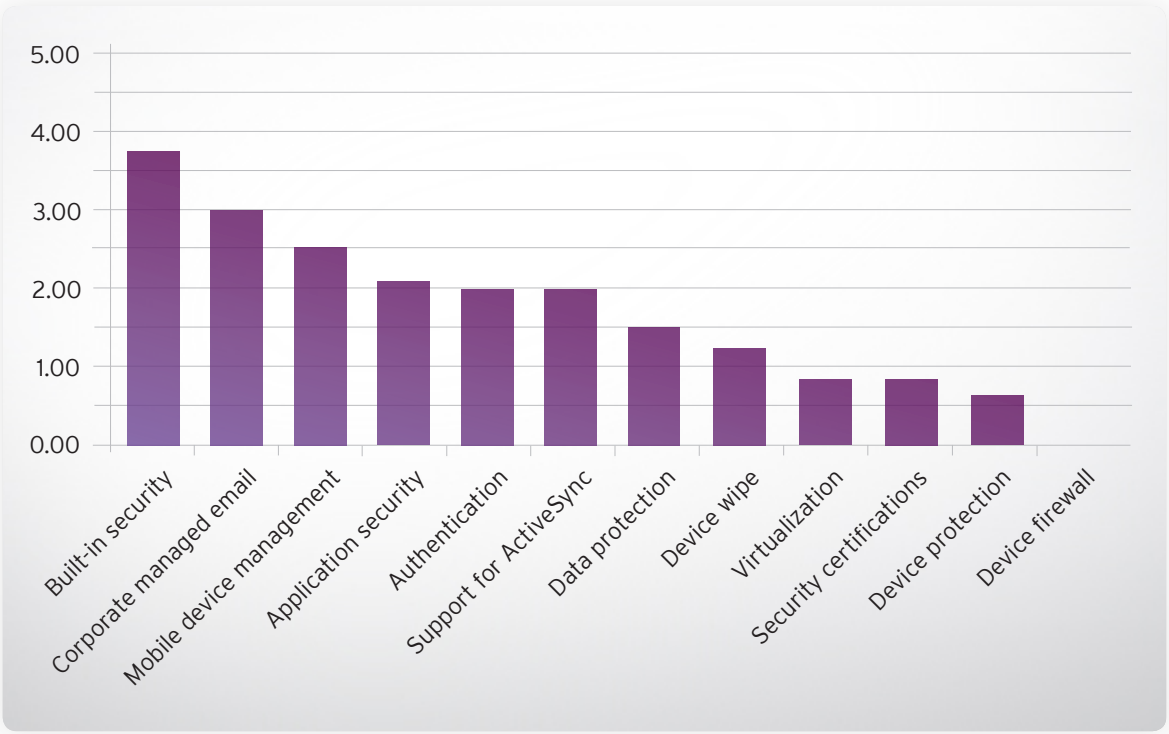

Figure 4 – Apple iOS Ratings

Google Android

Android has been designed from scratch, with security in mind. It is a privilege-separated operating system and applications can't access the network without prior consent. Apps run in their individual sandboxed environment, and permissions are granted by the user on a per-app basis. Unfortunately, the end user often fails to closely inspect the permissions request dialogue in their haste to use the app and, for the average end user, it is unclear when permissions are given and what the application is actually capable of. Once the application is installed, the OS doesn't recheck with the user and goes on to use the permissions without prompting the user again. This model, while theoretically more secure than the common sandbox on Apple iOS, has the net effect of putting each user in charge of their own security, rather than the operating system. The latest version of Android 4.x does include full device encryption for data protection and Address Space Layout Randomization (ASLR) for buffer overflow protection; however the fragmentation of the handset market means that Android 2.x is still the most widely deployed and provided on the majority of new handsets. Another side effect of this market fragmentation is that there is no central means of providing operating system updates. Security patches are provided to customers by individual carriers or handset manufacturers. There is an unacceptable delay in this process, meaning that many consumers remain unprotected from critical vulnerabilities for a prolonged period.

Android is currently the preferred platform by cybercriminals. With clever social engineering, they convince a victim to install a "useful" application. The user willingly gives permission, and bingo—the device is compromised. Premium SMS fraud Trojans are a costly reminder of unfriendly apps, but what is worse is the data exfiltration function of some of the digital nightmares—malware can copy SMS, intercept calls, remotely activate the microphone, or conduct other sinister tasks.

Attackers are using Android app stores as distribution mechanisms; they promote their apps through online marketing activities, which include sending out spam messages. This is facilitated through the lack of up-front validation of apps after they are submitted to app stores and before they are made available for download. It is compounded by the third-party app store functionality inherent in the Android app model. This open ecosystem is abused by the bad guys, and this will not stop until app store providers themselves establish strict reputation checking. Advising the user to only download from a trusted source does help to mitigate some of the risk, but this also has a downside. Users tend to see the official Android Market, now called Google Play, as a trusted source, yet multiple examples of malicious code are regularly found being distributed through this official channel. Effective social engineering often makes it complex to figure out if the publisher is a good one or a bad one. The responsibility is with the app store provider, and we hope to see stricter controls there. Google recognized this, and introduced Google Bouncer on the 2nd of February 2012 to "bounce" malicious apps, but there are still unfriendly apps in their store. Other market places don't provide "digital hygiene" yet. Due to this, we might see malware issues similar to those we see on Windows platforms, perhaps not traditional self-replicating worms, but certainly Trojans. If Android app store providers don't act soon, we could see over 120,000 malicious Android apps by the end of 2012.

Let's tighten the controls on the Android ecosystem a bit to ensure that this great flexible operating system stays safe and does not become the next "Microsoft Windows"—where you can't survive without an anti-malware program.

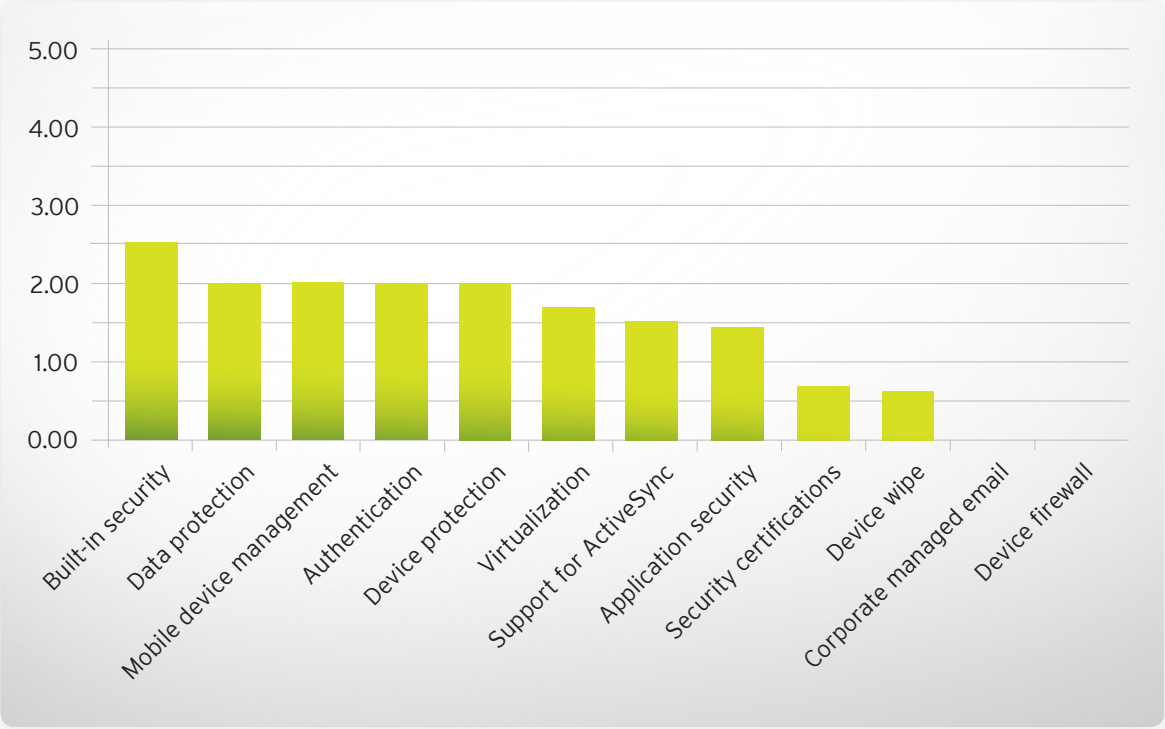

Figure 5 – Google Android Ratings

Microsoft Windows Phone

In many respects, it seems that Microsoft has learned the lessons of the past and created a reasonably robust and secure smartphone operating system with Windows Phone.

The OS uses a security model similar to the Android platform, in that minimum privileges and isolation techniques are used to sandbox processes or, in Windows Phone terminology, to provide chambers that act as individual process spaces. These chambers are created and implemented based on a policy system that, in turn, defines what system features processes operating in a chamber can access.

Features that may reveal a user's location or provide a source of private information are called capabilities on the Windows Phone. The Least Privilege Chamber has a minimal set of access rights that are granted by default but these rights are dynamic and can be expanded by using capabilities during the application install. These capabilities are granted during the install process for an application and cannot be elevated during runtime. This reduces any likely attack surface area and ensures that an application discloses all of its capabilities to a user. It achieves this by publishing its capabilities on the application details page in the Windows Phone Marketplace, prompting the user during the process of purchasing the application and when the user is about to use the location capability of the application and device for the first time.

Windows Phone does not support the use of removable data storage media, and the SD slot in the device is only for use by the original equipment manufacturer (OEM). If a hardware manufacturer does provide removable media then the phone will lock the media using an built-in 128-bit key that, in turn, will pair the phone with the removable media, preventing its use in another phone or PC.

The Microsoft Marketplace Hub contains applications that have been submitted by developers who have registered with the application development program. Windows Phone and the Xbox games systems are the only platforms from Microsoft that require the pre-approval of applications before users can run them, despite developers trying to create unofficial apps for the platform. These attempts were subsequently thwarted by Microsoft as they persuaded the developers of ChevronWP7 to withdraw their tool. Developers receive a certificate as part of the registration process as all applications are signed by VeriSign—unsigned applications are unable to run on a Windows Phone. The registration process includes an identity check for each developer registering with the program. During upload of applications to the Marketplace Hub, content, function, and compliance checks are made on each application against Marketplace policies that maybe in place.

Applications can be revoked in cases of serious security issues or in less severe cases updates can be sent out to users. Applications are developed using managed code, which combined with isolation of applications and the use of a least privilege model, supports the Windows Phone security model. The application security model prevents the Windows Phone Internet Explorer from installing applications and bypassing this model.

None of the major anti-malware vendors were reported seeing any significant malware targeting Windows Phone.

The next few months are critical for Microsoft and the Windows Phone. The product has been overshadowed by the likes of iPhone and Android devices, but with the current issues facing RIM, Microsoft has an opportunity to win over disgruntled users—especially within existing Microsoft shops. Of course the key driver, alongside consumer passion, is apps. Creating sufficient market demand is difficult if developers aren't writing apps for your platform, and that leads to a vicious cycle that is tough to break. The hope is that Microsoft will find their developer program mojo and build a successful ecosystem, but only time will tell.

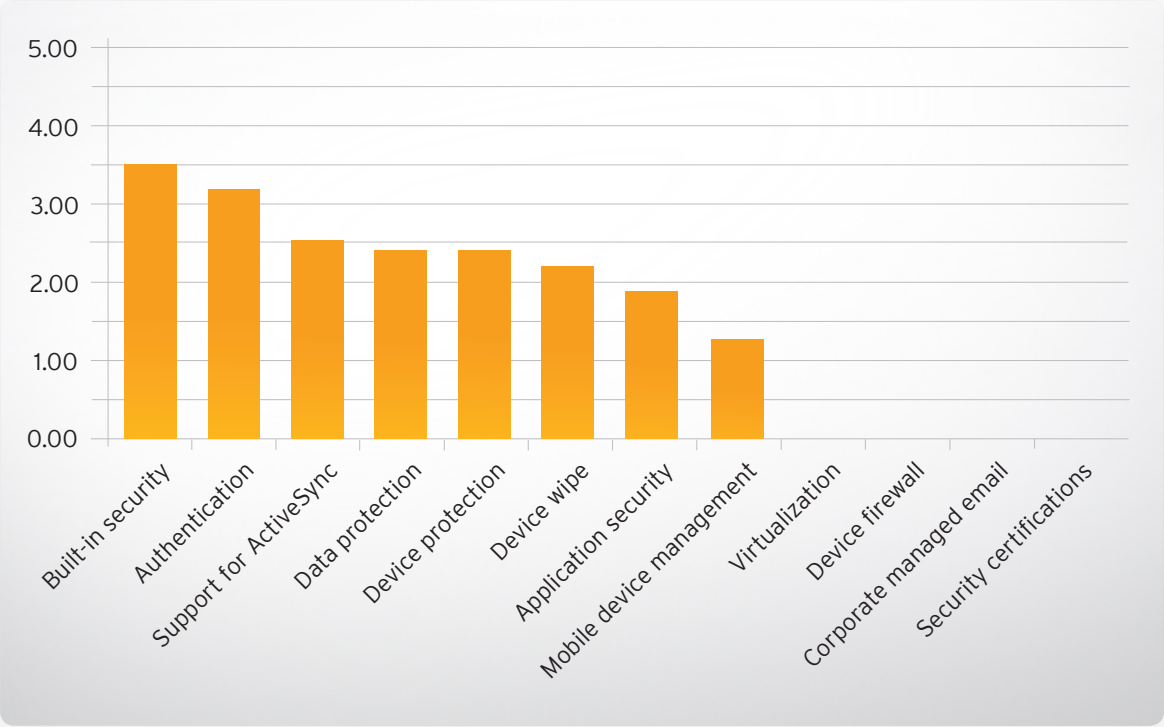

Figure 6 – Microsoft Windows Phone Ratings

Appendix – Security and Management Criteria

Note: NB Android 2.3 is used for comparison as it is the dominant installed/supplied version.

ID	ATTRIBUTE	BB 7.0	iOS 5	WP 7.5	ANDROID 2.3
1.00	**Built–in security**	**3.13**	**3.75**	**3.50**	**2.50**
1.10	Code signing	5.00	5.00	5.00	5.00
1.20	Keychain	2.50	5.00	0.00	0.00
1.30	Buffer overflow protection	2.50	2.50	4.50	2.50
1.40	Stack overflow protection	2.50	2.50	4.50	2.50
2.00	**Application security**	**2.44**	**2.06**	**1.88**	**1.44**
2.10	Centralized app signing	4.50	2.50	0.00	1.00
2.11	Developer app signing	4.50	2.50	4.50	1.50
2.20	Centralized application testing	3.50	2.50	4.00	1.00
2.30	User "allow" model	4.50	5.00	2.50	4.00
2.40	Anti-malware built in	2.50	4.00	4.00	2.00
2.41	Anti-malware support via open APIs	0.00	0.00	0.00	2.00
2.50	Web reputation built in	0.00	0.00	0.00	0.00
2.51	Web reputation via APIs	0.00	0.00	0.00	0.00
3.00	**Authentication**	**3.90**	**2.00**	**3.20**	**2.00**
3.10	Power-on authentication	2.50	2.50	4.50	2.50
3.20	Inactivity time out	5.00	2.50	4.50	2.50
3.30	SIM change	2.50	0.00	0.00	0.00
3.40	Password strength requirements	5.00	2.50	4.50	2.50
3.50	Protection from too many log in attempts	4.50	2.50	2.50	2.50
4.00	**Device wipe**	**4.00**	**1.25**	**2.25**	**0.63**
4.10	Local wipe – after too many failed login attempts	4.50	2.50	4.50	0.00
4.20	Remote wipe – over IP	3.50	2.50	4.50	2.50
4.21	Remote wipe – over SMS/cellular	3.50	0.00	0.00	0.00
4.30	Selective wipe	4.50	0.00	0.00	0.00
5.00	**Device firewall**	**4.50**	**0.00**	**0.00**	**0.00**
5.10	Over Internet Protocol (IP)	4.00	0.00	0.00	0.00
5.20	Over Short Message Service (SMS)	5.00	0.00	0.00	0.00
6.00	**Data protection**	**3.80**	**1.50**	**2.40**	**2.00**
6.10	Data at rest – encryption	5.00	2.50	4.50	0.00
6.20	Data in use – file separation	0.00	2.50	2.50	2.50
6.30	Data in motion – VPN, 802.1X	5.00	2.50	5.00	5.00
6.40	Remote backup services prevention – iCloud	4.00	0.00	0.00	2.50
6.50	Removable media – SD/USB SIM	5.00	0.00	0.00	0.00
7.00	**Device protection**	**3.50**	**0.63**	**2.38**	**2.00**
7.10	Jail breaking/Rooting	1.50	0.00	3.00	0.00
7.20	Patching – OS/Apps	3.00	0.00	4.50	3.00
7.30	Over-the-air (OTA) updates of the OS	5.00	2.50	2.00	5.00
7.40	Block access to untrusted certificates – SSL	4.50	0.00	0.00	0.00

Appendix – Security and Management Criteria (Continued)

Note: NB Android 2.3 is used for comparison as it is the dominant installed/supplied version.

ID	ATTRIBUTE	BB 7.0	iOS 5	WP 7.5	ANDROID 2.3
8.00	**Corporate managed email**	**3.42**	**3.00**	**0.00**	**0.00**
8.10	Remote account removal	2.50	3.00	0.00	0.00
8.20	Email forwarding prevention	4.50	3.00	0.00	0.00
8.30	Cross-in-box email move prevention	0.00	3.00	0.00	0.00
8.40	Applications use preclusion	4.50	3.00	0.00	0.00
8.50	Cut and paste preclusion	4.50	3.00	0.00	0.00
8.60	S/MIME email authentication and encryption	4.50	3.00	0.00	0.00
9.00	**Support for ActiveSync**	**0.00**	**2.00**	**2.50**	**1.50**
9.10	Number of policies supported – latest ActiveSync	0.00	2.00	2.50	1.50
9.20	Number of policies supported – legacy ActiveSync	0.00	2.00	2.50	1.50
10.00	**Mobile device management**	**3.50**	**2.50**	**1.25**	**2.00**
10.10	Richness of the API	2.00	2.50	0.00	1.50
10.20	Vendor-provided server	5.00	2.50	2.50	2.50
11.00	**Virtualization**	**0.00**	**0.83**	**0.00**	**1.67**
11.10	Virtual native OS	0.00	2.50	0.00	0.00
11.20	Virtual native apps	0.00	0.00	0.00	5.00
11.30	Split-user profile	0.00	0.00	0.00	0.00
12.00	**Security Certifications**	**2.50**	**0.83**	**0.00**	**0.67**
12.10	Federal Information Processing Standard (FIPS) 140-2	2.50	2.50	0.00	2.00
12.20	Evaluation Assurance Level (EAL) 4	5.00	0.00	0.00	0.00
12.30	FDA approval	0.00	0.00	0.00	0.00
	OS Average Score	**2.89**	**1.70**	**1.61**	**1.37**

Contributors:
Rik Ferguson - Director of Security Research and Communications, EMEA, Trend Micro
Cesare Garlati - Vice President, Mobile Security, Trend Micro
Raimund Genes - Chief Technology Officer, Trend Micro
Chris Silva - Mobile Industry Analyst, Altimeter Group
Nigel Stanley - Security Practice Leader, Bloor Research