SOPHOS

Mobile Security Showdown

iPhone, BlackBerry, Android—selecting the best device for your business

With its finely ingrained policies, BlackBerry remains the go-to mobile device for security-savvy enterprises. But iOS and Android devices are quickly catching up. The inclusion of fundamental enterprise security features such as full device encryption and Microsoft Exchange Active Sync compatibility makes iOS and Android powerful business tools—when properly configured, of course.

Make no mistake, iOS and Android devices are popular because the focus is on developing attractive features for the consumer mindset. That will continue to guide the development of new features on both platforms. But the adoption of fundamental security features makes them acceptable choices in an enterprise environment, and are driving the adoption of bring your own device (BYOD) policies.

Mobile security comparisons

When it comes to mobile platform security, BlackBerry is the most mature device. But enterprise readiness also adds to its complexity. Administrators can enable detailed solutions, but they take longer to implement. Also, without the BlackBerry Enterprise Server (BES) of a third-party MDM solution, BlackBerry offers very few personal management features.

The Apple iPhone can be described as "so far, so good" but it is not yet perfect for the enterprise. Its configuration tools are mostly intuitive, but the iPhone lacks a granular way of controlling applications. In addition, it does not provide the ability to remotely provision, configure, audit, or enforce devices without the use of Apple's server operating system.

Android has only recently arrived in the enterprise following the platform's 4.0 release, often referred to as the "Ice Cream Sandwich" release. It now includes full device and external memory encryption and a framework that allows for remote configuration management and third-party MDM solutions.

While the iPhone and BlackBerry are susceptible to malware, it is Android that is most frequently targeted by malicious apps. According to SophosLabs, there has been a 4,000% increase in the number of Android malware samples between 2011 and 2012.

As an IT administrator, you should be aware that permitting any specific device platform into your enterprise comes with risks. We can help you make an informed decision.

The following tables feature full comparisons of iPhone, BlackBerry and Android security features including application settings, policy management, and transport security.

Application settings

Feature	iPhone	BlackBerry	Android
Remote wipe	Remote wipe for iPhone is available through: ‣ Exchange 2007 Management Console ‣ Exchange 2013 Management Console ‣ Outlook Web Access ‣ Exchange ActiveSync Mobile Administration Web Tool ‣ Exchange 2003 - Exchange ActiveSync Mobile Administration Web Tool	Remote wipe is a core feature of the device and can be triggered from the BlackBerry Enterprise Server (BES). Wipe times and implementation are comparable to the iPhone 4S.	Remote wipe is available to any application, such as Google Sync, which uses Exchange ActiveSync or an application which chooses to use the device configuration framework and become a device administrator.
Encryption	iPhone 3GS and later and iPad devices have hardware encryption which is also enabled via the ActiveSync option. Pre-3GS devices do not provide encryption. Rumored encryption bypass vulnerabilities on some models all require the iPhone to be already jail-broken.	BlackBerry devices provide encryption and policy from the BlackBerry Enterprise Server (BES). The implementation is trusted and validated by many government organizations.	Android 3.0 and higher provides full file system encryption, so all user data can be encrypted in the kernel using the dmcrypt implementation of AES128 with CBC and ESSIV:SHA256. The encryption key is protected by AES128 using a key derived from the user password, preventing unauthorized access to stored data without the user device password.
Provisioning	Requires local configuration using iPhone configuration utility	Remote and local provisioning	Remote and local provisioning (through administrative apps)
Remote restore	No	Yes	Partially, if the account information is backed up to Google servers
Password	Partially, if the account information is backed up to Google servers	Rich policy management of password complexity comparable to a desktop environment	Passcode rules can be enforced using the device administration API, including: ‣ Screen lock type ‣ Minimum password length ‣ Fine grained password complexity ‣ Password expiration ‣ Maximum failed logon attempts

Policy management

Feature	iPhone	BlackBerry	Android
Enforcement	Can deploy a profile to an iPhone, and requires password authentication to override.	Can set strong controls for the device with a per-option policy on what can and cannot be edited by users. Flexible, but rather complicated.	Any app that has a permission to use the device administration API has the ability to change the policy. The app may set a policy as to what options can be edited by users.
Audit	No management or audit functionality currently available	Yes, based on policy; logged locally and centrally	No management or audit functionality currently available
Patching	Patches cannot be pushed over the network automatically. They are deployed by iTunes when the user connects and opts to update. iTunes cannot be centrally managed, so an admin cannot dictate deployment of the patch. Relies on user awareness.	Patches can be deployed remotely from the BlackBerry Enterprise Server (BES). Full patch audit status and management can be executed remotely without user intervention. When a reboot is required, policy can drive whether the user is given a choice to delay to a later time.	Patches cannot be pushed over the network automatically. They are deployed by Google, the device manufacturer and the mobile network provider.
Updates	Updates to profiles can be pushed remotely only by third-party MDM frameworks. They can be applied in the background without user interaction if the MDM client application has been granted administrative access.	Updates can be pushed from the BES remotely and applied in the background without user interaction.	Updates to profiles can be pushed remotely only by third-party MDM frameworks. They can be applied in the background without user interaction if the MDM client application has been granted administrative access.
Application control	Profiles can be set to restrict deployed applications. This occurs at bootstrap, (e.g., the administrator cannot deploy additional applications remotely). In-house applications can be developed for the device, which, in turn, are checked and signed by Apple.	The BES provides the ability to package and deploy specific applications remotely. Restrictions can be placed on applications that the user is allowed to install to a corporate white list or for administrator deployment only. Per-application policies can be set and managed remotely to limit application access to resources (e.g., network access, local data, permissions to change settings, use location). Extremely granular.	Application control can only be done using an MDM framework.
User rights management	By default a set of restrictions are provided: explicit content, Safari, YouTube, iTunes, allowing a user to install apps, allowing use of camera, screen captures.	Granular policies can be set, though they are somewhat intimidating.	Requires storage encryption, disables camera.

Transport security

Feature	iPhone	BlackBerry	Android
VPN	Password-based and token-based authentication available. Requires user interaction.	Provides encrypted tunnel back to BlackBerry Enterprise Server (BES) for data transfer. Also supports explicit VPN.	Password-based authentication. Requires user interaction.
Remote management	No	Yes	No
Email	Supports SSL across a range of protocols. Depends on server configuration (Exchange by default). Also allows the use of authentication certificates.	Supports by default through encrypted tunnel or directly to mail host.	Supports SSL across a range of protocols. Depends on server configuration (Exchange by default). Also allows the use of authentication certificates.
Proxy	Can set up proxy at the carrier's access point. All traffic can be forced through the VPN, which can be configured to go through a proxy.	Can set proxy policy at the BES level (routing all traffic back to the central server and routing through a single point). Can also set per-connection policies.	Proxy cannot be changed by the user or by an administrative app. All traffic can be forced through the VPN, which can be configured to go through a proxy.
Certificates	Includes the ability to use an SCEP server to control the issuing and revocation of certificates to the device. It is possible to create a profile containing certificates separate to using the SCEP server.	Can manage certificates and deploy remotely.	Some applications like Cisco AnyConnect VPN app include the ability to use an SCEP server to control the issuing and revocation of certificates to the device. It is also possible to distribute certificates manually or via URL.

For more information on mobile device management, be sure to visit our mobile security hub at Sophos.com.

United Kingdom Sales:
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales:
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia & New Zealand Sales:
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Boston, USA | Oxford, UK

A Sophos Article 11.12v1.dNA

SOPHOS