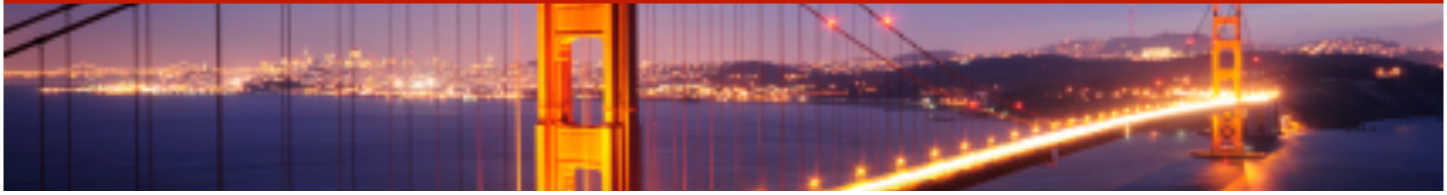
May 2009

Successful Mobile Deployments Require Robust Security



By: Maribel D. Lopez

FIRMS MUST BUILD SECURITY-ENABLED MOBILITY

Mobility is no longer considered a luxury within enterprise but a critical part of a networking strategy as firms look to increase productivity and remain competitive in a rapidly changing environment. As mobility becomes an integral part of the infrastructure, IT must deal with supporting numerous devices including laptops, smartphones and other mobile handhelds. The challenge for IT will be enabling productivity improvements while mitigating the risk of numerous types of devices. The devices and their memory cards may hold sensitive organizational and personal information, including information about product announcements, financial statements, or customer records.

In the PC world, IT can standardize on a platform. But in the mobile domain, IT must support numerous types of hardware and software including various versions of Windows Mobile, RIM BlackBerrys, Apple iPhones, Symbian devices, Palm devices and Linux-based devices such as Google's Android phones. These handhelds, which are now approaching the capabilities of laptops, create unique security requirements because these devices are:

- Often purchased and owned by the end user (with the exception of BlackBerrys which are often purchased by the firm)
- Lost more frequently than laptops but not immediately reported as lost
- Less likely to be protected by a strong passcode if purchased by an end user

IT must reduce the threats associated with loss, theft and malicious attacks on new mobile devices. IT departments have already established corporate security solutions and wireless security deployments should extend these practices. Given the unique aspects of mobile devices, such as limited processing power, storage limitations and the need to manage power consumption, IT must build solutions that are mobile-aware. For example, removable storage in mobile devices represents an additional security vulnerability that must be secured. As a result of these challenges, leading IT shops are already focusing on mobile security and manageability from the initial design phase through deployments. As IT incorporates mobility into its existing security policy, they should:

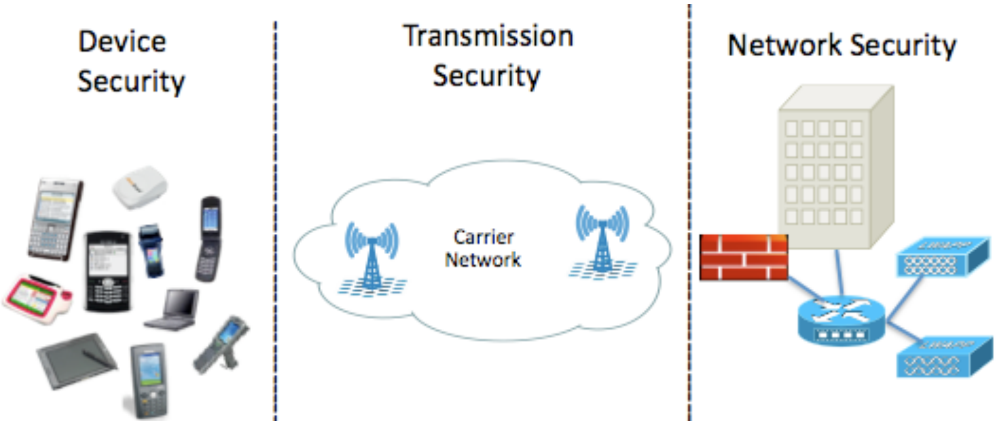
- Review the use cases of existing users
- Assess current and future mobile application usage
- Define security policies tailored for the corporate function of each user

Companies have varying degrees of security requirements. Firms that aren't using business applications on mobile devices may believe that a lower level of security is more acceptable, while others may consider the loss of email and contact information a security risk. But while access to e-mail may provide a lower risk of data loss than a CRM database, e-mail can also contain sensitive data in both the e-mail's contents and its attachments. With this in mind, firms should consider email as an application that also requires a robust security solution. For example, a firm may have liability exposure under data-protection law if a device is lost –even if the device only contains e-mail. Mobile security solutions must strike a balance between minimizing risks while remaining as transparent to the user as possible. For example, an end user will not type in a 20-digit password into a smartphone, but a 6-digit password containing both alpha and numeric digits is more reasonable.

DEFINING THE COMPONENTS OF A MOBILE SECURITY SOLUTION

A mobile security solution must take into consideration what types of applications will be used, what kind of data will be stored on the device as well as what regulations the firm is required to support (i.e. Sarbanes-Oxley Act (SOX), Gramm-Leach-Bliley (GLB), and Health Insurance Portability and Accountability Act (HIPAA)). A comprehensive mobile security solution provides protection on three levels by preventing unauthorized access to: 1) the device and its data 2) data as it transits the network and 3) the corporate network .

Figure 1. The three components of mobile security protection



1) The device and its data (Device security)

This refers to securing data that resides on the device as well as securing the device itself from malware. Best practices are that all data on the mobile device and any removable memory should be encrypted. In addition to encrypting data, a security solution should also minimize malware threats such as viruses, trojans and worms. There are two methods for securing the device. A firm will most likely need to use both if they are running a mixed environment. The first is to select devices that minimize malware risks by preventing unauthorized application downloads and restricting what an application can access without permission. The second is to add third-party software that includes both antivirus software and firewall software. Some devices such as RIM's BlackBerry already have an embedded firewall in the device and robust strategies against malicious code.

2) Data as it transits the network (transmission security)

A data transmission security solution enables identity verification of the sender and the receiver and protects data from being modified by a third party as it transits the wireless network. A firm can achieve this by encrypting the data using AES or Triple DES with an encrypted SSL tunnel. A cryptographic shared key system can be used to authenticate the sender and receiver. Firms should also look for solutions that support standards such as S/MIME, PGP and Lotus Notes native encryption to enable sender-to-recipient confidentiality, integrity, and authentication.

3) The corporate network (Network access security)

The third area of mobile security is protecting the corporate network. A robust mobile security solution must prohibit unauthorized access to the corporate network while permitting authorized users to pass data in and out freely. This function is made more complex by the fact that most IT organizations have a variety of firewalls, intrusion detection systems, and authorization systems, all of which must be coordinated to provide this function. Some techniques mobile phone vendors use to secure smartphone access back into a corporations' networks include VPN tunnels to gateways (Windows Mobile) and running data through a secure NOC to a server (RIM).

SECURITY SOLUTIONS VARY BY VENDOR

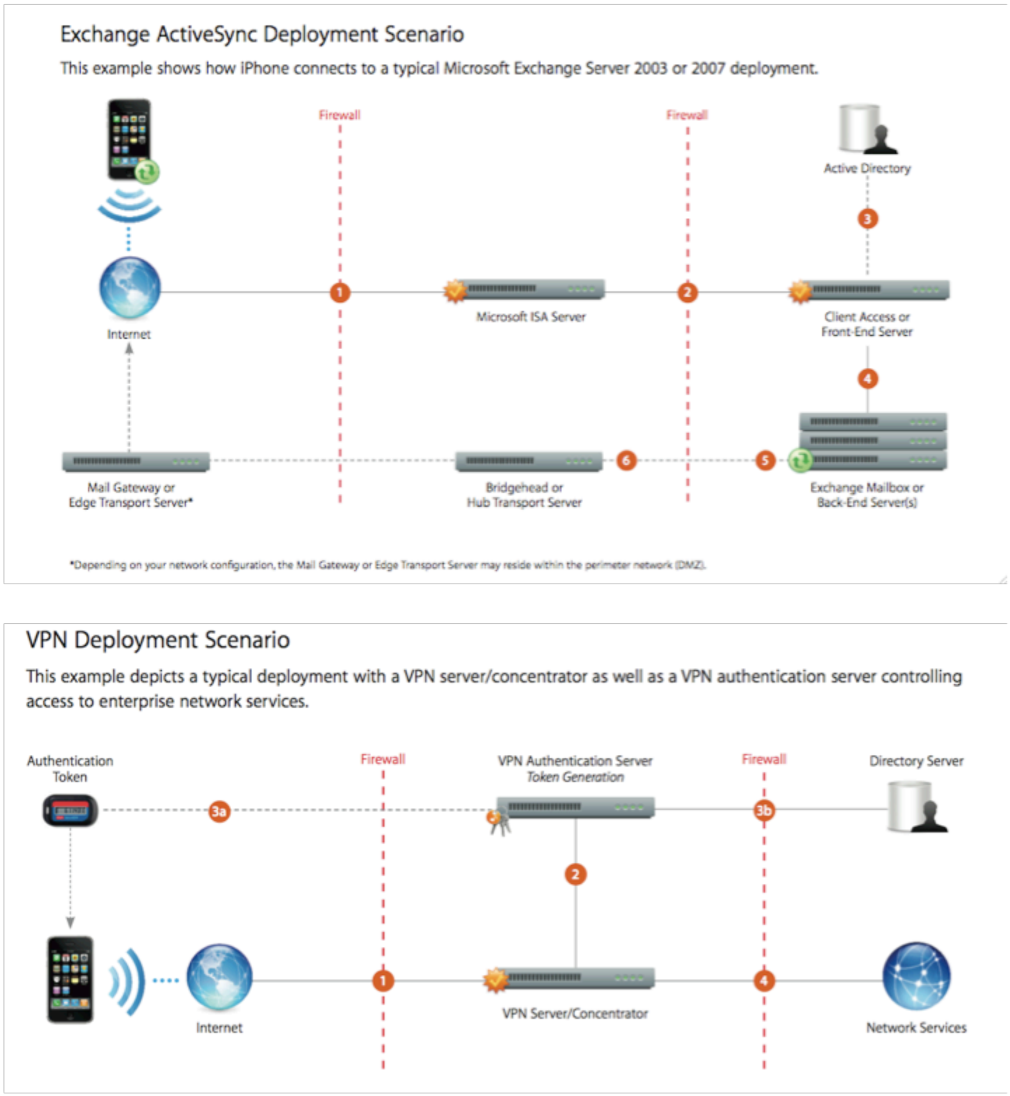
Just as the security requirements vary by company, the solutions that are offered vary by mobile device manufacturers and mobile operating system vendors. To provide examples of the differences in the various offerings, Lopez Research has provided a synopsis of the security offerings of Apple, RIM, and Windows Mobile. Given Nokia's recent shutdown of Intellisync and its retrenchment on the consumer marketplace, Lopez Research did not cover the Symbian OS in this report. Google's Android platform was also not evaluated since this platform is considered solely consumer-focused at the time of this writing. This research was conducted in the first quarter of 2009.

Lopez Research used the three levels of security listed above as a framework for evaluating and providing comments on the security implementations of the three mobile OS systems listed above. The following comments are designed to provide firms with a basic overview of the security solutions and should not be considered a comprehensive review of each vendor's security.

Apple's iPhone

Originally developed as a consumer product, the Apple iPhone is finding its way into corporations. As a result, Apple has added support for enterprise features using products from Microsoft and Cisco. Apple uses Microsoft Exchange ActiveSync to deliver push email, calendar, and contacts. For security, Apple supports Cisco IPsec, LT2P and PPTP Virtual Private Network (VPN) protocols, two-factor token authentication, as well as certificate authentication (see Figure 2). The latest release added remote wipe, password policy enforcement from ActiveSync, as well as WPA2 and 802.1x wireless security.

Figure 2. The Apple iPhone solution for ActiveSync and VPN deployments



Exchange ActiveSync Deployment Scenario

This example shows how iPhone connects to a typical Microsoft Exchange Server 2003 or 2007 deployment.

Firewall
Firewall
Active Directory
3
Internet
1
Microsoft ISA Server
2
Client Access or Front-End Server
4
Mail Gateway or Edge Transport Server*
Bridgehead or Hub Transport Server
6
5
Exchange Mailbox or Back-End Server(s)

*Depending on your network configuration, the Mail Gateway or Edge Transport Server may reside within the perimeter network (DMZ).

VPN Deployment Scenario

This example depicts a typical deployment with a VPN server/concentrator as well as a VPN authentication server controlling access to enterprise network services.

Source: Apple

Table 1. Rating Apple's iPhone for device, transmission and network security

Type of Security	Commentary	Rating by category
Device	• **Operating system can be compromised** • **lacks on device encryption** • **lacks OTA updates**	○
Network	• **Uses the same active directory based authentication methods as Windows mobile**	◕
Transmission	• **Full VPN support, but lacks the extra protection of a gateway or NOC server solution**	◑
Overall Mobile Security Rating	**Version 2.0 added several enterprise security features but the platform still lacks several basic yet critical features.**	◔

The iPhone uses secure read only memory (ROM) in the hardware of the device that contains cryptographic keys, which are used to validate the bootloader and the OS. This protects the bootloader and OS from modification or corruption. The OS also verifies the digital signatures in applications to confirm that they have been accepted by Apple for execution on the iPhone and have not been altered. However, hackers have designed Jailbreak software that allows users to bypass Apple's security system. Jailbreaking is a process that allows root access to the entire Unix file system. Once the device is jailbroken, the above safeguards to the device are compromised.

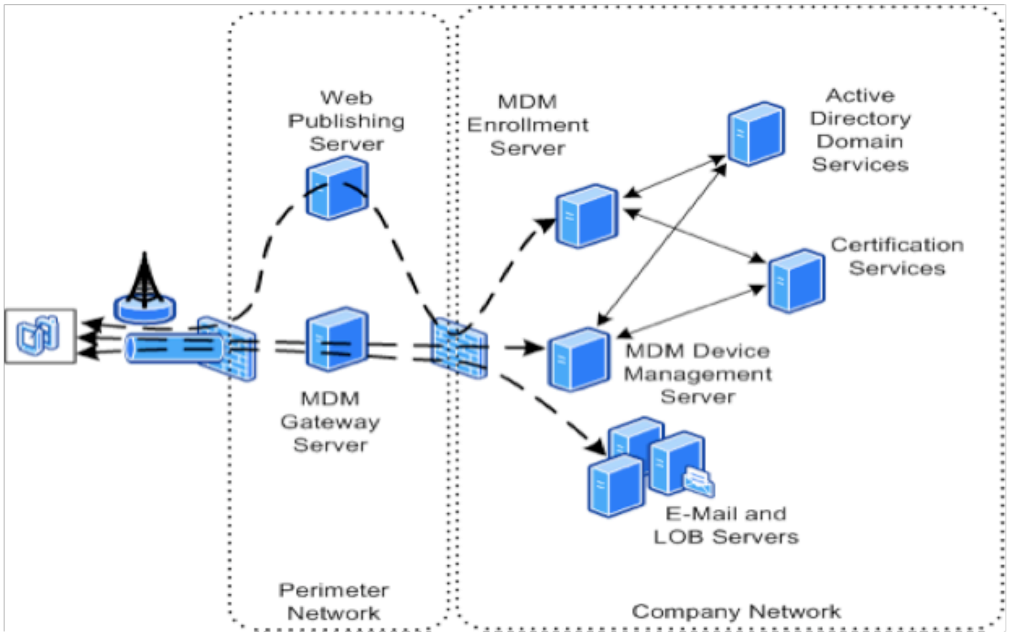
Apple now offers an iPhone Configuration Utility that can be used to set pass code policies as well as configure a users' VPN, email, and wireless network settings. However, the iPhone configuration profile is an XML file that the user must download from a web site or install from an attachment sent by IT in an email.

Overall Assessment: The original iPhone had numerous security holes that were improved by the July 2008 release such as remote wipe, password policy enforcement and VPN. However, the iPhone OS still suffers from a major security vulnerability, which is called jailbreaking. Jailbreaking allows the user to modify iPhone's file system. The software lets the user unlock the phone and download any applications they desire. This allows the user to bypass Apple's security and management systems, rendering the phone susceptible to security threats such as malware and hackers. In addition, the platform still lacks critical security features such as on device data encryption and over the air firmware updates. As a result, the iPhone security solution fails at the first line of defense, which is device level security. Vulnerabilities, such as using the emergency call feature to gain access to the home deck, are still being discovered. It also relies on third-party vendors to supply security at other levels such as VPNs. Overall enterprises should proceed with caution and limit the use of iPhones, especially for sensitive data.

Microsoft's Windows Mobile

Microsoft's security solution includes the Windows Mobile OS, System Center Mobile Device Manager (MDM) 2008, the MDM Gateway server and the MDM client application (only available on Windows Mobile 6.1 or later) that lets you manage the device through MDM. Microsoft doesn't build its own devices. All access to the company intranet is through the MDM Gateway Server that sits between the firewalls in the DMZ (see Figure 3). The MDM Gateway Server is a stand-alone server, not domain-joined, which authenticates incoming connection requests by verifying that it was signed by a particular root certificate. Once a Windows Mobile device has been authenticated using the Active Directory Domain Service it can connect to MDM Gateway Server. Microsoft uses a mutually authenticated SSL connection between the MDM Device Management Server and the MDM Gateway Server to protect against unauthorized network access.

Figure 3. Microsoft's Mobile Device Manager Solution



Source: Microsoft

To minimize malicious software or viruses on mobile devices, MSFT can use Active Directory Group policy to support application approval and blocking. On smartphones, WM offers two-tier access for code execution control where the executable runs only if it is signed with a trusted certificate and has been granted permissions.(Pocket PC only offers a single tier.)MDM security model requires X.509 certificates. Firms can use security policies to help control the acceptance of unsigned attachments, applications, or files. Microsoft uses AES encryption and an IPsec tunnel between the MDM Gateway Server and the Windows Mobile device to secure and encrypt communications over the carrier's network or a public Wi-Fi network. Using the MDM's software distribution, an IT manager can extend the existing AD Group policies out to the windows mobile devices.

Table 2. Rating Microsoft's Windows Mobile for device, transmission and network security

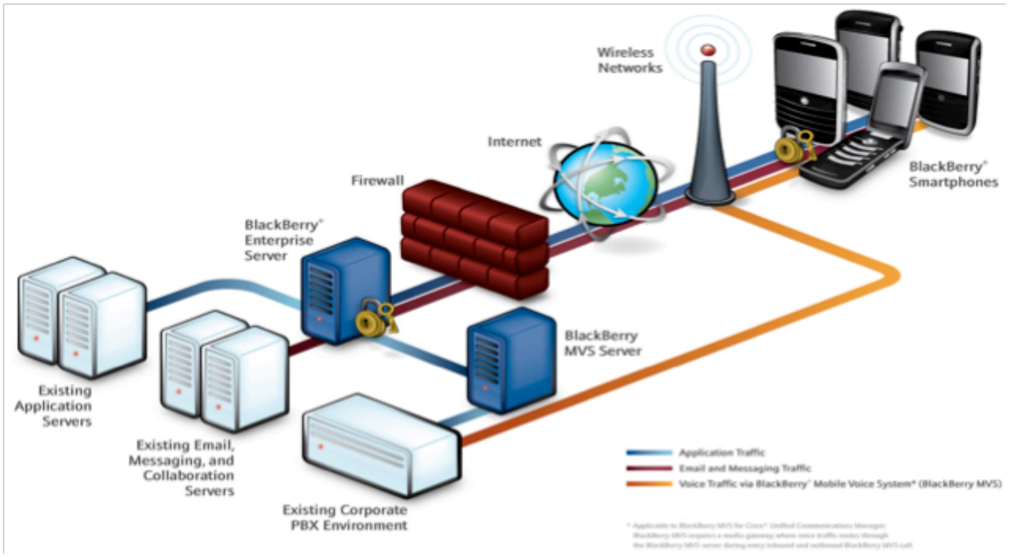
Type of Security	Commentary	Rating by category
Device	• **two-tier access for code execution control** • **removable storage but not on device encryption** • **supports OTA updates** • **requires third party Anti-virus and Firewall support**	◐
Network	• **Certificate and active directory domain services for authentication**	◕
Transmission	• **Full VPN support but provides MDM gateway in the DMZ**	◕
Overall Mobile Security Rating	**The Windows MDM security update covers a majority of firms' basic security requirements.**	◕

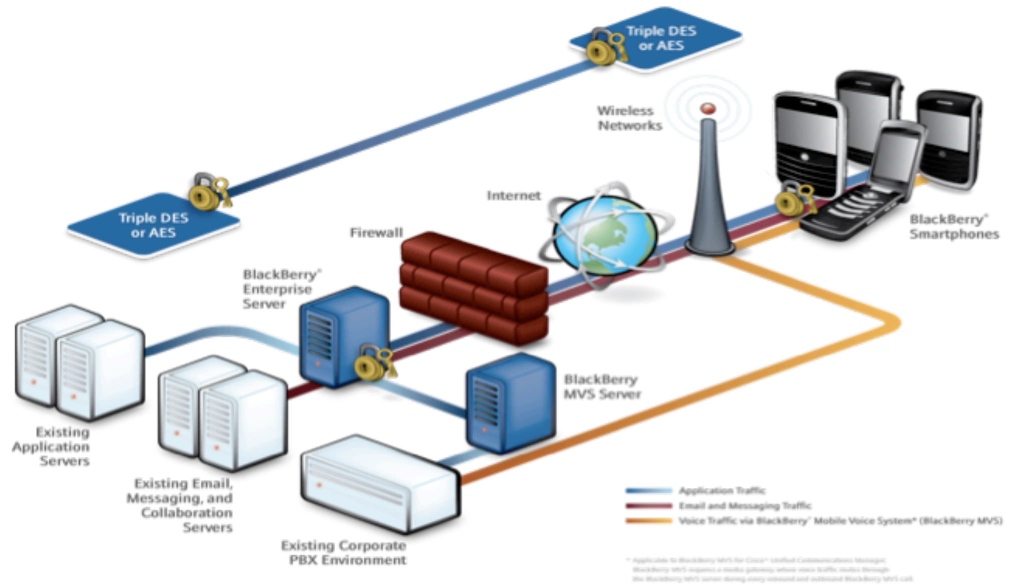
Overall Assessment: Microsoft has made progress in building a better security solution. Microsoft's solution leverages the existing infrastructure, such as Active Directory, to manage Windows Mobile capable devices meaning IT can manage the system with familiar tools and capabilities. Windows Mobile provides a solid solution for the device security and supports encryption for data in transit. Prior to the announcement of MDM companies had to open an SSL port on the firewall to allow encrypted data to pass through to the exchange server. This was considered unacceptable by many firms and inhibited the adoption of Windows Mobile. Now traffic connects to the network via the MDM server, providing a better solution for corporate network security. It also recently achieved common criteria certification EAL 2+ for Windows Mobile 6.1 in August of 2008. The combination of MDM and a VPN provide a reasonable security solution for firms that would like to use Windows Mobile devices.

RIM's BlackBerry

The BlackBerry architecture is a fully integrated solution from one vendor that includes the device and its OS, the BlackBerry Enterprise Server (BES) and the Network Operations Center (NOC). RIM has built three levels of security into the product consisting of: 1) security within the device, 2) a secure connection between the device and the BES, and 3) a secure connection between the BES and the NOC (see Figure 4).

Figure 4: RIM's Security Solution


Wireless Networks
Internet
Firewall
BlackBerry® Smartphones
BlackBerry® Enterprise Server
BlackBerry MVS Server
Existing Application Servers
Existing Email, Messaging, and Collaboration Servers
Existing Corporate PBX Environment
Application Traffic
Email and Messaging Traffic
Voice Traffic via BlackBerry® Mobile Voice System* (BlackBerry MVS)
* Applicable to BlackBerry MVS for Cisco® Unified Communications Manager; BlackBerry MVS requires a media gateway where voice traffic routes through the BlackBerry MVS server during every inbound and outbound BlackBerry MVS call.


Triple DES or AES
Triple DES or AES
Wireless Networks
Internet
Firewall
BlackBerry® Smartphones
BlackBerry® Enterprise Server
BlackBerry MVS Server
Existing Application Servers
Existing Email, Messaging, and Collaboration Servers
Existing Corporate PBX Environment
Application Traffic
Email and Messaging Traffic
Voice Traffic via BlackBerry® Mobile Voice System* (BlackBerry MVS)
* Applicable to BlackBerry MVS for Cisco® Unified Communications Manager; BlackBerry MVS requires a media gateway where voice traffic routes through the BlackBerry MVS server during every inbound and outbound BlackBerry MVS call.

Source: RIM

RIM secures the device from the time it powers on. The Boot ROM checks the authenticity of the Java Virtual Machine (JVM) and the OS. The JVM then checks the integrity of the device software. If either check fails, the device will not boot. The BlackBerry software and JVM can't be accessed by other applications. The system is designed so that data remains encrypted at all points between the BlackBerry device and the BES. RIM supports PKI. It also supports both S/MIME and PGP, sender-to-recipient security solutions, which ensures that the message cannot be read or modified anywhere along the way. Mutual authentication and transport encryption between the device and the BES provides confidentiality, integrity and authentication without requiring a separate VPN.

Some companies have expressed concern that the NOC provides a single point of failure and/or they are uncomfortable with certain data transiting through a foreign country. However, all messages sent through to the NOC are encrypted using Triple DES or AES-256 encryption and all messages are encrypted with keys, that are stored only in the BES and the device. Neither RIM nor the operators have access to the customer keys and therefore cannot see the content of any of the messages. As a result of these procedures, this fear has waned as the most security conscious groups such as financial institutions (i.e. Citigroup) and government agencies (i.e. FBI) have embraced the RIM platform. RIM also claims the NOC reduces costs by amortizing the cost of multiple redundant connections to the carrier across all BES servers.

Table 3. Rating RIM's BlackBerry for device, transmission and network security

Type of Security	Commentary	Rating by category
Device	• Complete control of what can be executed on the device • On device and removable media encryption • supports OTA updates	●
Network	• Encrypts the message • Uses a cryptographic shared key system for authentication	●
Transmission	• Routes traffic through the NOC and the BES to ensure security • Doesn't require a VPN	●
Overall Mobile Security Rating	RIM provides solid security across the three areas of vulnerability.	●

Overall Assessment: Security was designed into the platform from its inception, including areas such as verifying the authenticity and the integrity of the device and its software. RIM offers strong security protection across the device, transmission and the network domains through tight control of the device, its software and its application control policies. RIM's BlackBerry was the first mobile solution to be certified under the Common Criteria Scheme. The product also has the most security certifications globally including FIPS 140-2, CAPS, EAL-2+, Coverity and Fraunhofer. While other vendors have stepped up security efforts in the past year, RIM offers the most robust security solution.

Conclusion

There is no one size fits all mobile security solution. A firm must decide how much confidential data will be on its users' devices and build a solution that maps the rigorousness of the security to the data risk. These security policies should be similar to a firm's laptop policy but take into consideration the differences in the devices' ability and the user's tolerance for security. IT should expect its end users to have different device preferences. This means it is unlikely that a firm will use a single mobile vendor or a single OS for all of its smartphones. Therefore, IT must understand the differences in the security implementations of each vendor and attempt to provide a consistent level of security across platforms.