

# Creating a Business-Class Mobility Environment in the Enterprise



by Eugene Signorini and Phil Hochmuth | February 2010

## Executive Summary

Enterprise employees want to bring their own devices to work and integrate them with corporate messaging systems and applications. This trend puts enterprise IT at a crossroad: Allowing this practice may open new opportunities for worker productivity and availability, but it potentially introduces security risks and IT support headaches. Blocking usage of personal smartphones might give enterprises a sense of security and control, but smartphone users often find work-arounds and hacks to circumvent IT controls they feel limit their personal productivity. Instead, enterprises can take advantage of the best that consumer smartphones have to offer while minimizing risk by building an IT network and applications infrastructure that provides an inclusive yet controlled and secure environment for both corporate-owned and employee-owned smartphones and mobile devices. This report outlines considerations and best practices for enterprises looking to build such a business-class environment.

## Table of Contents

I. Consumerization of the Enterprise Marches On	2
Methodology	3
II. Balancing End-User and IT Requirements	3
Understanding the Needs of Mobile Workers	3
Understanding the Requirements of IT and Management	4
Reconciling Conflicting Technology Needs	5
Potential Stifling of Innovation Through IT Lockdown	6
III. Defining the Business-Class Mobility Environment	6
Enterprise-Strength Smartphone Fundamentals	7
Device-Level Security and Policy Management	8
Network Security and Policy Management	9
Integration with Mobile Middleware and Device Management Platforms	9
IV. Conclusions and Recommendations	10
Recommendations	10

This custom publication has been sponsored by Research In Motion.

## I. Consumerization of the Enterprise Marches On

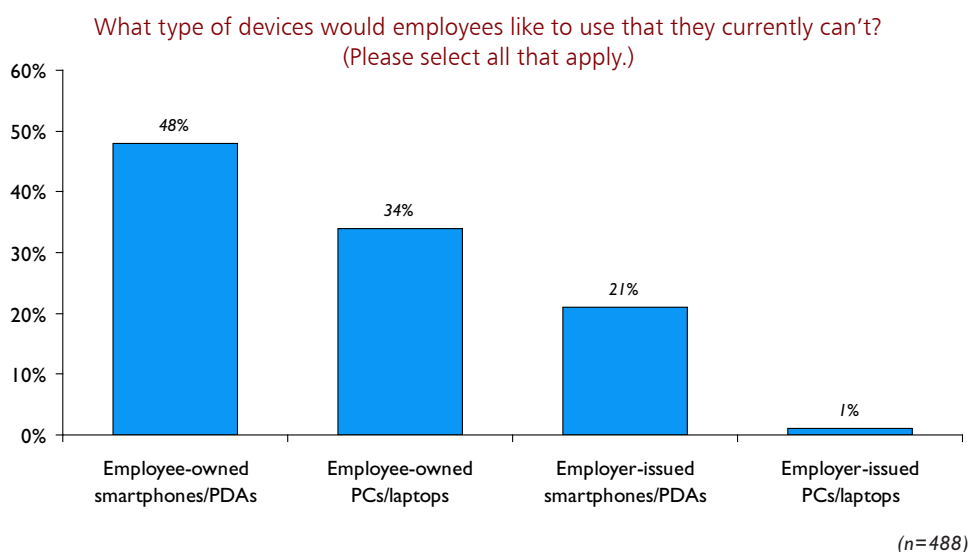
The line between consumer-focused and business-focused smartphones is blurring as devices such as the iPhone become more common as work tools and adoption of devices such as Research In Motion's BlackBerry increases among regular consumers. Enterprises are already inundated with such devices, and there is no end in sight, as the Droid smartphone and Google's own Nexus One hit the market. The draconian reaction to all this is the lockdown/lock-out of non-corporate smartphones from enterprise use—banning access to corporate e-mail, applications and internal networks from employees' personal devices. This approach is short-sighted, however, and it risks alienating end-users and forcing some to find technical work-arounds (which can lead to increased

IT headaches and possible data security issues). The alternative, allowing these devices to access corporate applications and networks, is just as perilous. Untested devices may be incompatible with corporate applications and security standards, and the thought of valuable corporate data and information floating around on thousands of employee-owned devices is the nightmare of any chief information security officer or risk and compliance executive.

As shown in Exhibit I, almost half of enterprise employees want to use their personal smartphones to access corporate networks, but current IT restrictions prevent them from doing so. Instead of locking out personal technology, enterprises would do better if they harnessed the capabilities of these powerful devices while at the same time managing and securing them.

### Exhibit I: Employees Want To Bring Their Own Devices to Work

Source: Yankee Group's Anywhere Enterprise—Large: 2009 U.S. Transforming Infrastructure and Transforming Applications Survey, Wave 1-12



## Methodology

Yankee Group was commissioned by Research In Motion (RIM) to conduct an independent assessment of the consumerization of enterprise mobility. In this report, Yankee Group uses research it conducted independently of RIM, including the following syndicated surveys:

- Anywhere Enterprise—Large: 2009 U.S. Transforming Infrastructure and Transforming Applications Survey, Wave 1-12
- Anywhere Enterprise—Large: 2009 U.S. Empowered Employee Survey, Wave 1-12
- Anywhere Consumer: 2009 U.S. Survey Suite, Wave 1-12
- Yankee Group's Link Data: North America Consumer Forecast, December 2009

We also rely heavily on one-on-one conversations with five enterprise IT and business decision-makers in the areas of mobility and security.

## II. Balancing End-User and IT Requirements

It's clear from the above highlighted trends that businesses are already in the throes of the consumerization of enterprise mobility. It's also clear that businesses can benefit from mobile technologies—even those that are being procured by end-users. What isn't entirely clear to IT leaders is how they can effectively manage mobility initiatives if this trend continues unabated. The first step is understanding the needs of mobile workers and the requirements of IT and management when it comes to wireless technologies. From there, business leaders can better determine the policies and frameworks to put in place to balance end-user and IT needs.

### Understanding the Needs of Mobile Workers

The needs of mobile workers can best be described as technologies that enhance productivity (most employees do indeed want to be productive) but at the same time provide flexibility (especially when it comes to work-life balance). Yankee Group uses the term "empowered employee" to describe workers who embrace technology for both productivity and flexibility; when it comes to the tools and technology they seek out, these workers will naturally migrate to solutions that provide both.

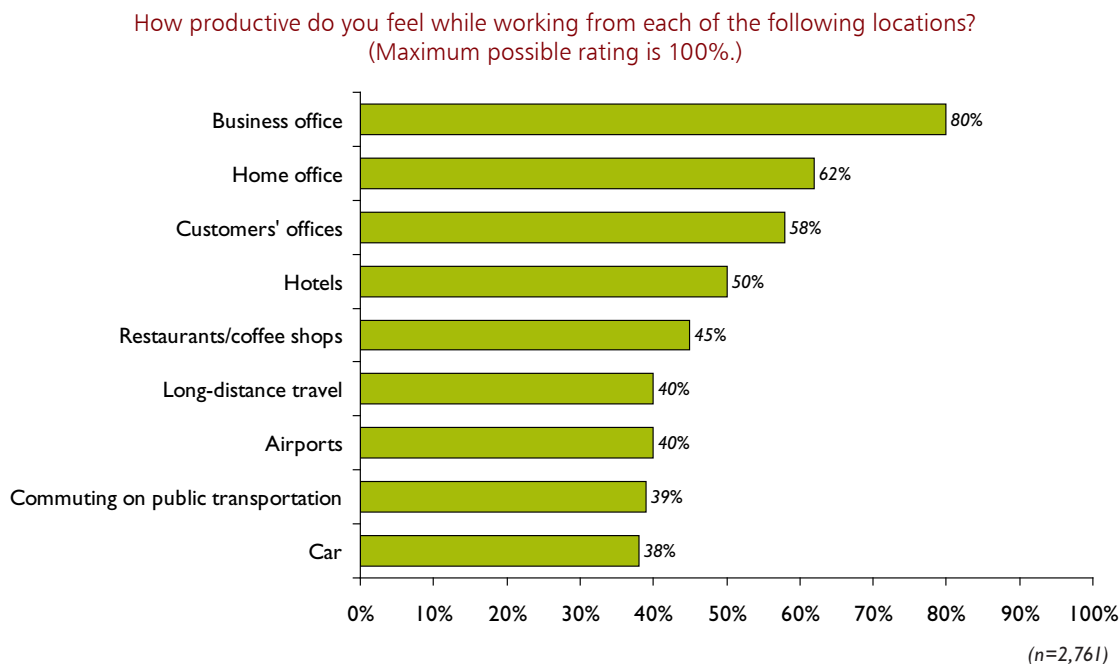
End-users are increasingly migrating to consumer applications, not just for personal use, but for business purposes also. According to Yankee Group's employee survey, 49% of end-users either already use consumer applications for business purposes or would be interested in doing so. Consumer instant messaging (51%) and consumer e-mail (49%) applications lead the way, but users also have heavy interest in mobile picture/photo messaging (29%), Web-based productivity applications (28%) and social networks (23%). However, 52% of end-users say their IT departments prevent them from downloading such applications.

The most-cited reason behind respondents' desire to use consumer applications for business purposes is that they are "already familiar with these applications from their non-work life" (44%). This highlights the growing blending of consumer and business lifestyles perfectly. When dealing with this "blended lifestyle" issue, IT must also realize that different technologies require different approaches. With laptops and PCs, for example, IT has been dealing with encroaching consumerization largely by taking a restrictive approach. Smartphones are new territory, however, and IT departments will likely need to take an alternate tack. Most employees view their smartphones as truly personal devices, and progressive IT organizations are putting into place appropriate policies to allow more reasonable usage without compromising fundamental corporate requirements. The most successful policies will treat smartphones as equally important as laptops for business purposes, but also won't blindly apply laptop lockdown policies to manage them.

Support of mobility tools is especially important for enhancing worker productivity. Workers increasingly feel less productive when away from their business or home office. Exhibit 2 on the next page displays how employees feel when working from different locations; a score of 100 indicates the maximum level of productivity. It's easy to see that productivity begins to fall off dramatically once users move away from their business office to mobile locales. This would imply that enterprises have a significant opportunity to drive additional productivity through the use of appropriate business mobility technologies.

## Exhibit 2: Employees Need Greater Access to Mobility Tools to Remain Productive

Source: Yankee Group's Anywhere Enterprise—Large: 2009 U.S. Empowered Employee Survey, Wave 1-12



### Understanding the Requirements of IT and Management

The requirements of IT leaders can best be described as technologies that drive end-user productivity, but at the same time allow for control and manageability. When it comes to deploying new technologies, IT and management certainly seek those that can make their end-user constituents more productive; however, they tend to err on the side of technologies that are proven to be manageable and secure.

Given the state of the economy, it is no surprise that IT and business leaders are placing a premium on driving maximum productivity throughout their organizations. Our infrastructure survey shows that driving operational efficiencies (cited by 44% of respondents) and streamlining/automating business processes (cited by 38%) are the two biggest priorities for IT. Other initiatives such as achieving more customer focus (26%), collaboration with customers (17%), mobile worker support (12%) and worker-to-

worker collaboration (10%) fell further down the list of priorities. While IT obviously wants to improve productivity, these results show a disconnect from what end-users want: Mobility and worker collaboration fall low on IT's priority list, but wireless tools such as smartphones and consumer applications such as IM and social networking are the technologies that end-users are seeking to enhance their productivity. No wonder end-users are taking matters into their own hands.

Of course, IT and business leaders are also very concerned about control, manageability and security. When asked to identify their primary concern when deploying mobile applications, respondents' top choice by far was "inadequate data security solutions" (44% of total respondents). But companies that don't prioritize technologies such as smartphones and mobile applications, instead allowing users to take matters completely into their own hands, expose themselves to much greater risks from security, cost and compliance standpoints.

## Reconciling Conflicting Technology Needs

Some of the benefits of employee-driven mobile device consumerization are becoming clear: the ability to be productive almost anywhere and a culture of openness for end-user technology preferences. Companies are also seeking ways to maximize returns on their current investments, and mobility is one way they can accomplish this. By taking advantage of smartphones already deployed in the organization, many of which were purchased by end-users themselves, an enterprise can realize business benefits with minimal additional investment.

However, this cannot be accomplished without organizations taking steps to ensure that these benefits aren't offset by the "bad" and "ugly" issues we outline in this paper's companion report, "Consumerization of the Mobile Enterprise." (Such issues include sprawl and complexity from various device OS types on the network, as well as issues of taxing businesses on the personal mobile phone usage of employees who have company-provided devices). We'll now look at the flip side of this equation—the risks and potential consequences of a business allowing its employees

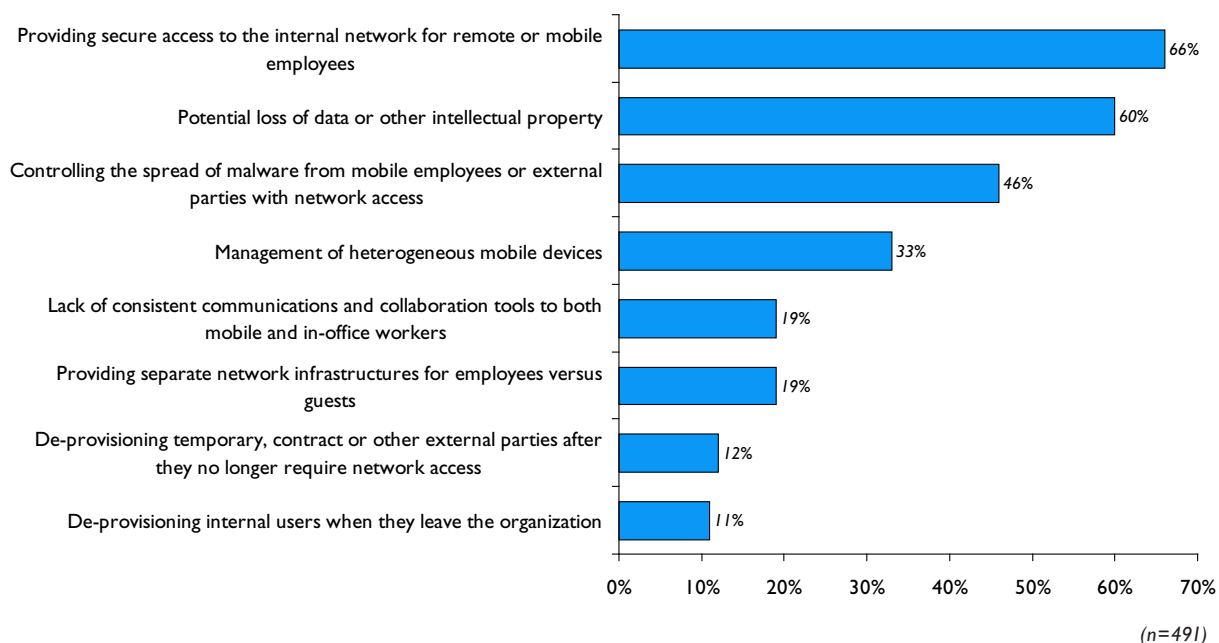
to get onto the network with the device of their choice. The issues facing enterprises go deeper than the potential management headaches and chaos of employees having gadgets outside of IT's control, potentially consuming network bandwidth, resources and, perhaps most importantly, the precious time of workers.

Fear of data theft or data loss is among the concerns related to having a more dispersed work force with access to applications and data from devices such as smartphones. According to Yankee Group's infrastructure survey, employee-owned smartphones are the top devices employees would like to use to access corporate network resources, but their IT departments do not allow them to do so. Fears about data security drive this (see Exhibit 3): 60% of enterprise IT leaders say the potential for data or intellectual property loss is among the top obstacles they face when expanding mobility options for employees, ahead of traditional security concerns, such as malware spread (46% said this was a top obstacle), and operational concerns, such as the management of heterogeneous mobile devices (33%).

### Exhibit 3: Top Concerns Among Enterprises with Mobile Work Forces

Source: Yankee Group's Anywhere Enterprise—Large: 2009 U.S. Transforming Infrastructure and Transforming Applications Survey, Wave 1-12

From a technology standpoint, what are the top three obstacles to providing and supporting these new mobile and remote computing options?  
(Please select up to three.)



Predictably, one of enterprise IT's biggest fears about the use of consumer devices at work is not what workers are doing with these gadgets, but what they might be downloading to them. Most personal smartphones with SD card storage can be plugged into a corporate laptop USB port and appear as an external drive to the PC. In an unsecured environment, workers can easily move sensitive data such as customer information, intellectual property or confidential files to their phones in order to have access to them while traveling, or simply to bring their work home with them—especially if they work on a stationary PC and don't have a corporate-issued laptop.

While some security industry rhetoric is likely responsible for data loss fears among enterprises, those organizations that have suffered from such events attest that the damage caused by such incidents is acute and real.

Overall, data loss incidents have risen over the last several years, increasing from 140 in 2005 to 703 in 2008, according to DataLossDB.org, a nonprofit firm that tracks publicly reported data loss incidents. While these incidents are still relatively rare when compared to other security breach events, the disruption and damage they cause are proportionally higher than their frequency. For example, according to Yankee Group's infrastructure survey, viruses were the most frequently experienced security incident in the last 12 months, with 78% of enterprises reporting an infection. Of those affected, 33% of enterprises say the infection either moderately or severely disrupted business operations. Only 9% of enterprises say they had corporate data stolen in the last 12 months, but among those who experienced this, 35% say the incident greatly disrupted business operations.

### Potential Stifling of Innovation Through IT Lockdown

Despite data loss fears, organizations that take a lock-it-all-down approach to data and the devices used to access it risk alienating the work force and stifling workers' abilities to be productive and innovative. According to Yankee Group's infrastructure survey, 40% of enterprise employees say their personal technology is more advanced than that offered by their employer; additionally, 56% of these employees say they are more productive when they have access to technology they use in their personal lives (e.g., non-IT-issued technologies such as collaboration apps, or personally owned devices such as phones or laptops).

The less-is-more security tack many enterprises already take toward endpoint control is a step in the right direction. According to Yankee Group's infrastructure survey, tight control over endpoints is a measure used to secure the usage of mobile devices—both employee- and company-owned—within the enterprise: 40% of enterprises say this is their most important security measure. However, strong identity management (58%) and policy-based network access controls (49%) are viewed as more important measures when securing mobile workers (see Exhibit 4 on the next page).

The most interesting aspect of this trend is the recognition that the onus is on the network, not the device, to act as the underlying security safeguard against data loss. This also means IT is already aware of the consumerization trend and has decided not to get into the whack-a-mole game of trying to secure, control or squash every new type of device that comes through the front or back door and onto the corporate network.

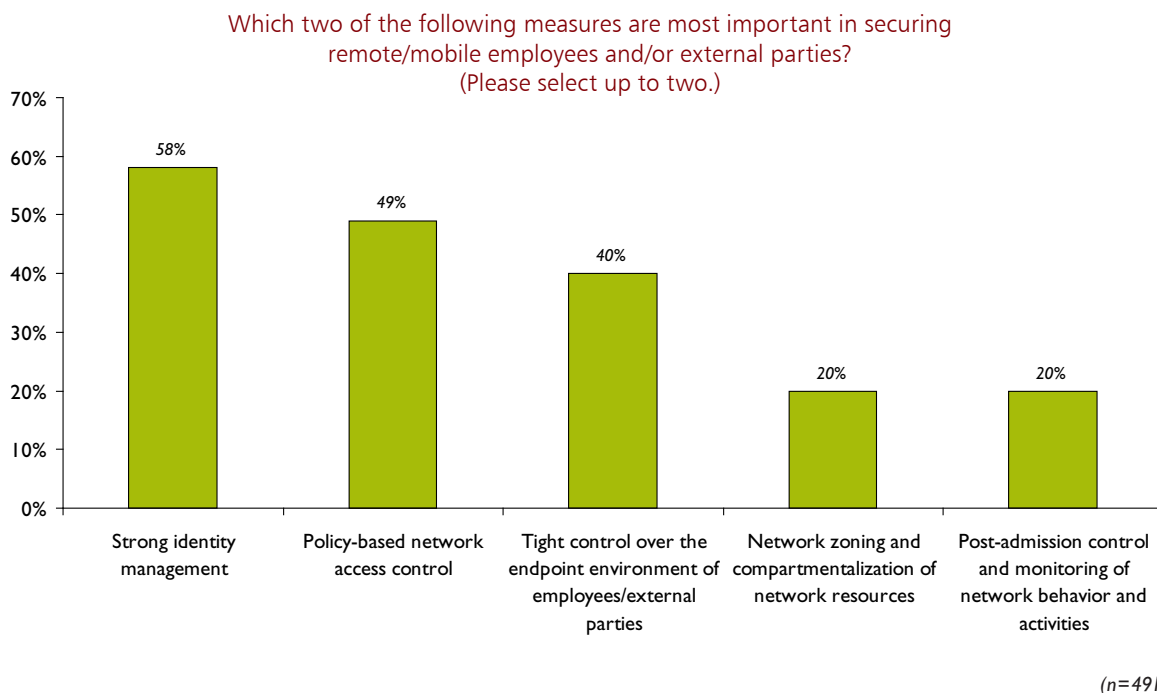
Security through selective access starts by giving end-users access to the core applications, tools and data resources they need so they won't go poking around and looking for things, potentially accessing or copying data they shouldn't see in the first place. In fact, enabling access to the full features allowed on traditionally locked-down devices often minimizes the need for organizations to support excessive multiple platforms or for individuals to carry additional devices.

### III. Defining the Business-Class Mobility Environment

So far, all of our guidelines and descriptions regarding how enterprises need to absorb consumer devices have leaned more toward the end-user side of the argument, with emphasis on empowering employees through more permissive device policies and inclusive access control methods. But we do not mean to imply that enterprise IT and security teams should cede all autonomy and control to end-users. The trend toward consumerization makes it clear that any smartphone or access device available in the general marketplace will ultimately find its way into the enterprise, whether it's authorized or not. However, not all devices are truly business class, and as IT and business leaders make the tough decisions about which devices and device platforms to support, they will find that some devices are just not ready for enterprise prime time.

## Exhibit 4: Identity and Access Control Are Preferred Over Endpoint Lockdown

Source: Yankee Group's Anywhere Enterprise—Large: 2009 U.S. Transforming Infrastructure and Transforming Applications Survey, Wave 1-12



Any device used to access sensitive business data and applications must be able to be managed and secured, ideally, out of the box. Policies don't matter if IT doesn't have the tools to implement them consistently across a broad range of devices. It is important for IT leaders to understand the characteristics that define business-class devices and platforms.

### Enterprise-Strength Smartphone Fundamentals

By fundamentals, we mean the core capabilities that most smartphones advertise and users take for granted. However, heavy-duty business users will test these features to their limits:

- **Long battery life:** Batteries must last at least a full day with heavy voice and data usage.
- **High-performing wireless radios:** These ensure the best quality service on whatever networks (wireless wide-area, WLAN) to which devices are connecting.
- **Durability:** The device must survive at least minor drops and excessive usage.
- **Broad messaging capability with strong user interfaces:** This includes access to not only corporate e-mail, but also calendars, to-do lists, etc.
- **Desktop-like applications:** Access must be provided for a reasonable range of functionality comparable to a desktop environment, including support for both corporate and consumer IM platforms, access to enterprise desk phones, unified communications applications and, increasingly, social media tools.
- **Multimedia capability:** This includes support for high-resolution cameras and video players.
- **Full HTML browsing:** The browser must be capable of showing any standard Web page at the same quality as a PC-based browser.
- **Accessory availability/compatibility:** Mobile professionals will demand a wide range of accessories and physical components as part of their device ownership, including extra cases, batteries and chargers. Minimizing the number of platforms supported can help address this requirement.

- **Accessories to support specialized roles, such as field service:** This includes hard cases, bar code scanners, credit card swipers, printers, etc.
- **Network coverage:** It should support multiple carriers, with global scale.
- **Basic iPhone-like features:** These include speakerphone, microphone, Bluetooth support and other capabilities.

IT leaders should proactively obtain and test the latest smartphones requested by their users. In most cases, key indicators of smartphone performance (such as battery life and radio quality) can only be determined through first-hand usage. Making evaluation even more complex is the lack of standardization. While there are industry standards for talk-time and standby, smartphones handle data and media differently, which can have a significant impact on performance.

## Device-Level Security and Policy Management

While much has been made of the blurring line between personal and work life, successful integration of consumer endpoints requires that a clear line of demarcation be drawn at some point. In order to implement policies around user access, IT must be able to control business-class devices at the feature and application level. This could include, for example, barring access to certain applications such as consumer instant messaging (for compliance purposes) or turning off device features such as video/still cameras. End-users' personal mobile devices, when used in an enterprise setting, should also include the support of a base set of security technologies, such as Advanced Encryption Standard (AES), which encrypts data over the air based on practically uncrackable 256-bit encryption keys, as well as password-protection and AES-level encryption of stored data on mobile devices. Also look for certified solutions that meet classifications such as Federal Information Processing Standard (FIPS) and the Common Criteria Evaluation and Validation Scheme standard—secure by government standards is more than good enough for enterprises. Mobile devices brought into an enterprise IT environment must support a set of technologies on the devices themselves, including:

- **User name/password:** Many enterprises don't require this feature to be enabled, but when employees' devices are brought into the workplace and used to access corporate IT assets and data, IT administrators should require use of this feature as a basic security safeguard for device access. Passwords should be required to be "strong"—defined as longer than 12 characters with a mixture of numbers, symbols, and upper- and lowercase letters. Additionally, the enterprise IT group must support remote device password resets in the event that an end-user forgets or loses his or her password.
- **Encryption and data management:** Endpoints must have the ability to support encrypted data on the device memory as well as on removable media (e.g., SD cards or other on-device storage). IT should also consider integration of mobile devices, or back-end mobile device middleware or management platforms, with enterprise data loss prevention software or enterprise rights management tools. Many organizations have made the significant investments required to classify sensitive data and write policy around its access and use; it would be a mistake not to extend these capabilities and safeguards to smartphones and employee-owned devices that might have access to corporate data stores.
- **Administrative "back-door" access:** Enterprise IT should have the ability to access and, in some cases, remove or alter the underlying applications, data and OS of an end-users' personal device. In extreme circumstances, this lets IT remove unwanted applications, data or even malware that could harm the network or other IT assets. Although this can be a touchy subject with end-users, evoking the image of Big Brother deleting personal applications or files from a smartphone, this is a trade-off that should be required of employees who want a tight level of integration between their personal devices and enterprise IT applications, directories and other network/IT resources.
- **Remote delete/wipe of devices:** Enterprises must be able to know what applications are present on employees' personal devices if those devices are to be used frequently in a business setting. The enterprise must have the ability to remove data from endpoint devices if an employee leaves the organization, or if a device is lost or stolen.

- **Compliance with the device's original hardware/software requirements:** Smartphones often come with device-maker- or carrier-imposed restrictions regarding the kinds of applications they can run or the types of mobile networks they are allowed to access. "Unlocked" or "hacked" devices are ones on which the owners have circumvented these technical restrictions by altering the phone's hardware or software. It is good policy to prevent end-users from integrating unlocked or personally modified devices into a corporate network or enterprise IT/application infrastructure. Such hacked devices are more likely to cause problems on the network.

## Network Security and Policy Management

As employees bring their mobile devices into corporate IT environments, they will likely access both corporate Wi-Fi and IP networks and carrier-run wireless wide-area networks. Enterprises can ensure the security of smartphone traffic by requiring devices to authenticate to an enterprise-class WLAN infrastructure. Beyond that, however, IT security should track the traffic behavior of these devices, which can be done via:

- **MAC/IP filtering and monitoring:** End-users who have SSID and WPA2 password credentials can still authenticate non-approved mobile devices to the WLAN. However, IT security can exert some control over these endpoints by identifying the MAC addresses of devices and allowing only a pre-defined access list of devices to get onto the network. Enterprises that are more permissive about network access for smartphones can monitor consumer-based devices by tracking device MAC and IP addresses, as well as by correlating existing access control lists with server and application access logs and network-based flow data (i.e., NetFlow or sFlow).
- **Network segmentation:** Instead of allowing employees to access an internal, secured WLAN via a personal mobile device, enterprises can set up separate WLAN subnets, or SSIDs, specifically for groups of personal mobile devices to gain Internet access. These subnets could be used to provision specific services for devices, such as Unlicensed Mobile Access (UMA) voice or VoIP/FMC services, or to allow access to resources such as internal mobile application servers or corporate "app store" sites. Another approach is to host corporate content (such as extranet sites or portals) or other IT resources in a demilitarized zone, as opposed to behind the corporate firewall.
- **Application auditing/classification:** When an employee brings his or her mobile device to work with the intent of integrating the device with corporate IT applications and networks, there should be an expectation that IT will have deeper visibility into the device than if the user were simply bringing a cell phone or employee-owned smartphone to work for personal use. To that end, an enterprise must have the ability to actively monitor the applications installed on an endpoint in order to ensure that unauthorized or potentially harmful applications aren't in use. If unauthorized or unwanted applications are running over the network, IT must have the ability to either remove the apps from the endpoint or block that endpoint's network access while the end-user is notified.

## Integration with Mobile Middleware and Device Management Platforms

This relates closely to a previous point: business-class devices must come with their own management tools (such as BlackBerry Enterprise Server) and/or integrate well with third-party mobile application/middleware and device management software platforms. These tools allow IT and policymakers to control access on devices, ensure that data is wiped from lost or stolen devices, and provide the means for enterprise-grade backup, restore and software-updating capabilities. Key attributes of strong device management platforms include:

- **Traffic visibility:** The ability to see and control what applications and data are coming onto and leaving devices.
- **Device transparency:** Visibility into device specifics such as version codes, battery status, carrier plans and data usage is also key to monitor for support purposes.

However, device integration with a back-end platform does not necessarily imply that the device allows for control at an application or feature/function level. It is critical that the chosen platform allows for device-level policy and security management at the level of granularity detailed above.

## IV. Conclusions and Recommendations

Managing consumer mobile devices in the enterprise requires delicate balance and a certain amount of permissive discretion. Organizations that are too permissive with employee-owned smartphones may have happy employees using personal tools, but this comes at the cost of exposing the company to security threats and a chaotic device management scenario. The extreme opposite of this scenario is one in which IT dictates the devices and applications used, but employees are unsatisfied with a tedious tool set that, in many cases, is inferior to their own personal technology. The ultimate goal is to find a balance where end-users can feel highly productive using both corporate and consumer applications that yield business benefits and provide work/life balance, while maintaining control of cost, security and compliance issues. In order to do this, organizations must understand what constitutes a business-class mobility platform that provides IT with the ability to manage and control certain critical components while allowing for worker flexibility.

### Recommendations

- **Strongly evaluate mobile middleware platforms and managed mobility solutions as part of a comprehensive mobility deployment.** Mobile application platforms represent a viable technology choice to develop, deploy and manage mobile applications to a diverse set of mobile devices and OSs. Managed mobility offerings also can assist procurement and finance in controlling the complexity of managing users across multiple carriers and rate plans. In general, such platforms can also help IT departments keep up with the expanding scale of their mobile device deployments.
- **Develop strong identity-based access control policies in the network.** When access is tied to who the user is, as opposed to the device he or she is using, IT security becomes simpler and endpoint options open up for employees. Securing end-users with consumer devices starts with securing the network and how people access it, as opposed to trying to control what's on the devices themselves. Enterprises with strong network-based controls for accessing applications and data can more easily absorb greater numbers of consumer smartphones.
- **Require a baseline set of security and remote management capabilities for mobile devices.** Enterprises that allow personal smartphones to enter a work environment—especially a corporate WLAN—must have some requirements for basic WLAN security and data management on the devices. Enterprises should establish a baseline set of security and management features that employees' personal devices must meet before they can be supported by enterprise IT.
- **Don't be afraid to just say no.** While there is a need for flexibility, in the end, organizations must avoid creating a Wild West environment where anything goes. Devices that don't meet defined criteria should not be funded, allowed network access or otherwise supported. IT organizations support limited desktop software; there is no reason smartphones shouldn't undergo similar scrutiny.

## Yankee Group—the global connectivity experts

The people of Yankee Group are the global connectivity experts—the leading source of insight and counsel trusted by builders, operators and users of connectivity solutions for nearly 40 years. We are uniquely focused on the *evolution of Anywhere*, and chart the pace of technology change and its effect on networks, consumers and enterprises. For more information, visit <http://www.yankeegroup.com/>.

Yankee Group has a global presence including operations in North America, Europe, the Middle East, Africa, Latin America and Asia-Pacific. Contact us at:

### Corporate Headquarters

One Liberty Square  
7th Floor  
BOSTON, MASSACHUSETTS 02109  
617-598-7200 phone  
617-598-7400 fax

### European Headquarters

56 Russell Square  
LONDON WC1B 4HP  
UNITED KINGDOM  
44-20-7307-1050 phone  
44-20-7323-3747 fax

## Yankee Group Link

Yankee Group Link membership brings clients the insight, analysis and tools to navigate the global connectivity revolution. It provides timely, actionable and accessible research and data that analyze the impact of connectivity and the transformation it will create in driving enterprises and consumers to an Anywhere society. The result is an experience that no other market research firm can provide.

### Link Research

Yankee Group's qualitative research forms the core of our offerings, with analysis focused exclusively on the transformational effects of the connectivity revolution. Our research reports arm you with the insight and analysis to make the right decisions today and tomorrow.

### Link Data

Yankee Group's quantitative data analysis includes monitors, surveys and forecasts. Together with Link Research, our data connects you to the information you need to make the most informed strategic and tactical business decisions.

### Link Interaction

Connect one-on-one with Yankee Group analysts to get answers to your most strategic and critical questions, as well as gain deeper insight into research and trends. We encourage you to have direction interaction with analysts through ongoing conversations, conference calls and briefings.

### Link Consulting

Who better than Yankee Group to help you define key global connectivity strategies, scope major technology initiatives and determine your organization's readiness to undertake them, differentiate yourself competitively or guide initiatives around connectivity change? Our analysts apply Yankee Group research, methodologies, critical thinking and data to produce expert, timely, actionable results.

### Link Events

The Anywhere revolution won't wait. Join our live debates to discuss the impact that ubiquitous connectivity will have on your future. Yankee Group's events—live and online—offer our clients new insight, knowledge and expertise to better understand and overcome the obstacles to succeed in this Anywhere revolution.

