CIO
Custom Solutions Group

Keeping Pace with Enterprise Mobility: A Step-by-Step Approach

As mobile manufacturers fall in and out of favor, companies must take a comprehensive look at every aspect of their mobility strategies.

SPONSORED BY
SAMSUNG

CIO
Custom Solutions Group

As only seems appropriate, enterprise mobility solutions and strategies can't stay in one place for very long. Given the rapid evolution of mobile devices, apps, platforms and services, enterprise IT and business departments must regularly revisit and fine-tune their activities in order to keep up with a highly fluid mobile market and user expectations. Understanding the need to adapt corporate strategies in response to – and in anticipation of – mobile market shifts is one thing. Identifying and implementing the best possible changes is another thing altogether.

The phenomenal growth of smartphone and tablet shipments and the shifting popularity of different mobile device brands make clear why enterprises must continually revisit their mobility strategies and policies. Two or three years ago, who could have known that, according to market research firm IDC, nearly 80 percent of the 236.4 million smartphones shipped in the second quarter of 2013 would be Android-based devices? Or that Samsung alone would hold nearly 40 percent of the Android smartphone market share?

Mobile device vendors that fail to innovate and, as a result, miss the mark on user demand, can quickly transition from market leaders to also-rans. These types of shifts can have a big impact on enterprises, especially given the widespread corporate adoption of bring-your-own-device (BYOD) policies.

Companies that support BYOD allow employees to use their personal mobile devices to access corporate resources and do work. A recent survey by IDG Enterprise found that more than half of the organizations surveyed already have BYOD plans in place. If corporate mobility policies don't reflect the changing profile of their employees' mobile devices, enterprise IT may quickly lose the ability to manage and control those devices effectively.

As earlier-generation mobile devices fall out of favor, and as mobility technologies evolve, enterprises need to follow a well-thought-out process to optimize their mobility strategies. That process, which this paper discusses, goes well beyond simply evaluating the functionality of any given mobile device. Also important are everything from employee preferences to partner ecosystems, along with the management and security requirements that typically top the list of concerns of CIOs and business executives alike.

STEP 1: ASSESSING MOBILITY NEEDS AND EMPLOYEE PREFERENCES

Any effort to initiate or fine-tune a mobility strategy shouldn't begin with a focus on mobile devices. Rather, the first step should be an in-depth assessment of the current mobility practices and processes already in place within the organization. In other words, before companies can determine how they can best use current-generation mobile devices and technologies, they first need to understand how mobility intersects with their core business objectives, and how their employees currently use mobile devices.

In many cases, there will be a generational element that comes into play in such evaluations. Younger workers who came of age in a world of pervasive social networking and mobility may suggest new use cases that can make them and their employers more efficient and productive. Simply swapping out old devices for new and changing

The Five Steps

☑ Step 1
Assess mobility needs and employee preferences

☑ Step 2
Ensure the mobile platform meets security and management requirements

☑ Step 3
Ensure the mobile platform has an extensive ecosystem of apps

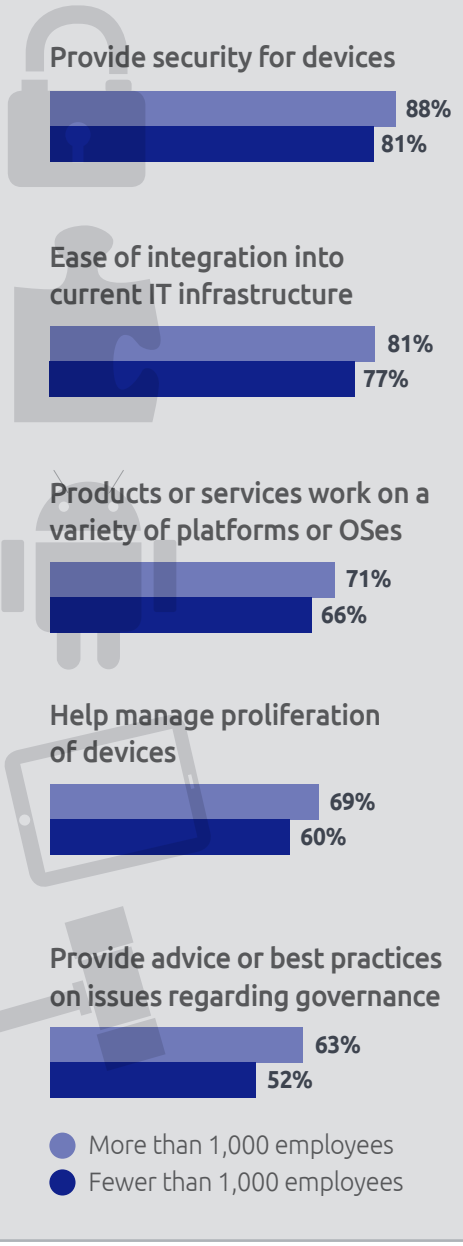
☑ Step 4
Ensure the mobile platform's vendor has an extensive partner ecosystem

☑ Step 5
Ensure the availability of required enterprise services and programs

CIO
Custom Solutions Group

Figure1. **Evaluating mobile technology vendors**

Factors considered critical or very important when evaluating mobile technology vendors



SOURCE: *2013 Consumerization of IT in the Enterprise survey*, IDG Eneterprise

little else can be a missed opportunity to optimize an enterprise's mobility operations based on the new platforms' capabilities and on new use cases and processes.

A key piece of this macro assessment is learning which mobile devices employees prefer. Companies that have instituted BYOD programs can get a good sense of these preferences simply by determining what types of personal mobile devices employees are bringing into the work environment.

Even when companies follow the traditional model of purchasing, distributing and supporting corporate-owned mobile devices, they should take employee preferences into account before deciding to adopt any given platform. If IT and business managers fail to determine employee preferences, they may discover that the devices they select are either rejected or underutilized.

Once companies have gained a good understanding of their existing mobility profile and their employees' mobile practices and preferences, they can move on to additional stages of the evaluation process. Failure to perform this first critical step can severely undermine the ultimate success of any evolving mobility strategy.

STEP 2: ENSURE THE MOBILE PLATFORM MEETS SECURITY AND MANAGEMENT REQUIREMENTS

Having completed an overview of their mobile environment and deciding where they want to take it, enterprises next must ensure they can manage and secure that environment and the corporate data within it. This step is usually high on enterprises' evaluation checklists. An IDG Enterprise survey of more than 1,600 IT and business managers and professionals found this to be the case. As illustrated in Figure 1, in that early 2013 survey, 88 percent of the respondents working at corporations with more than 1,000 employees said the ability to provide device security is an important factor when they evaluate mobile technology vendors. Among this group of respondents, 69 percent also cited the need for these vendors to help manage the proliferation of mobile devices.

As with Step 1, enterprises should begin this stage of their evaluation not with a focus on a particular device, but with an assessment of their organization's overall risk profile. Among the key questions an enterprise must answer:

- What corporate information and resources are especially valuable and/or sensitive?
- How can the company best balance the benefits versus the risks of providing mobile users access to corporate data and resources?
- Which corporate data can be downloaded to mobile devices and which needs to stay behind the corporate firewall?
- What types of security technologies and practices are available for mobile devices and mobile use cases?

Only after these and other risk-profile questions have been answered can organizations intelligently determine the level of security controls they require on mobile devices, in their mobile management systems and in their security policies.

CIO
Custom Solutions Group

Mobile device management (MDM) systems constitute a critical component of any enterprise security regime. These systems provide functions such as device provisioning, monitoring and, if necessary, remotely wiping corporate data from the devices. An MDM system must be flexible enough to apply existing company policies against current mobile device populations, as well as accommodate new policies and next-generation devices.

Once enterprises understand their mobile security needs and the capabilities and requirements of their management infrastructure, they can move on to evaluating device-specific security features. Any candidate mobile devices should work well with the MDM system and other management infrastructure, and should complement those centrally run systems with their own on-device security features. Those device features can include strong access controls, data encryption, device partitioning and other security and management capabilities.

STEP 3: ENSURE THE MOBILE PLATFORM HAS AN EXTENSIVE ECOSYSTEM OF APPS

Security and management won't matter much if a new mobile device can't run the applications you need. The target platform should have a large library of available apps for download, and should also be able to give users secure and simple access to centralized corporate applications. Having already conducted their risk assessment and security profile, enterprises will know what apps and data they will allow to run on the devices themselves, and which they will maintain as virtualized resources behind the corporate firewall.

Many companies may decide to establish enterprise app stores of approved apps for their mobile users, while blacklisting other apps that expose security vulnerabilities or other risks. Almost all mobile devices also come with preloaded apps from the device vendor and the carrier, and the IT department should evaluate the usefulness of these apps as well as their potential risks.

Beyond an assessment of the available packaged apps, enterprises should determine if the mobile device vendor or its partners offer a good portfolio of app development, migration and customization tools. This need was highlighted in the *2013 Consumerization of IT in the Enterprise* survey by IDG Enterprise. In that report, 41 percent of enterprise IT leaders cited "difficulties in making core enterprise applications available remotely" as a top mobile app challenge.

With such tools, the company or a contractor can migrate existing mobile apps to new platforms, customize apps to meet specific business needs or create new apps from scratch.

STEP 4: ENSURE THAT THE MOBILE PLATFORM'S VENDOR HAS AN EXTENSIVE PARTNER ECOSYSTEM

When enterprises evaluate mobile devices, they also need to evaluate the ecosystems of partners that support those devices. Unlike consumer purchasers, corporations often require systems integration and consulting services to plan and deploy

CIO
Custom Solutions Group

THE DEVICE PARTNER ECOSYSTEM should include a good selection of systems integrators and consulting firms. These partners, collectively, should be able to deliver general mobility business services as well tailored services that meet the individual and industry-specific needs of your enterprise.

comprehensive mobile solutions, as well as complementary products (such as MDM systems) to manage and enhance the operation of the mobile devices themselves.

Among the most important of these ecosystem partners are app vendors whose software offers needed functionality while also leveraging features that may be unique to the candidate mobile devices. While some app vendors will offer standard business solutions, others may offer industry-specific apps that address critical vertical-sector needs. A good partner ecosystem will have a large community of both types of app vendors and solutions.

Given the potential complexity of enterprise-wide mobility programs, as well as the need to customize them to individual company requirements, the device partner ecosystem should also include a good selection of systems integrators and consulting firms. As with the mobile apps, these partners, collectively, should be able to deliver general mobility business services as well tailored services that meet the individual and industry-specific needs of your enterprise. The geographic coverage of these ecosystem partners should also match up well with the geographic distribution of the enterprise and its employees.

In the same way, the partner ecosystem should include companies able to deliver worldwide distribution and support services for those enterprises that need it. If regional offices or employees need services such as training, break-fix-replace device services or other support offerings, having local partners can significantly affect mobile efficiencies and productivity.

STEP 5: ENSURE THE AVAILABILITY OF REQUIRED ENTERPRISE SERVICES AND PROGRAMS

More prosaic than device and data security, but also critical from an IT and business perspective, is the need to easily and cost-effectively maintain and service mobile devices throughout their corporate life spans. Basic mobile device warranties typically run just one year, whereas the devices themselves may be in use for three years or more over their corporate lifetimes. Companies require flexible and extensible warranties and service plans to ensure global business continuity, to maintain and enhance productivity, and to reduce device management expenses and improve ROI.

Service plans may include on-site or off-site device service, programs to rapidly replace lost or broken devices and a number of other enterprise-focused features. As with the partner ecosystem, these plans should provide for worldwide coverage that matches well with the enterprise's own geographic distribution.

Samsung – Meeting the full range of enterprise mobility needs

As it grew to become a leading mobile device provider worldwide, Samsung committed itself to meeting the wide range of requirements that enterprise customers bring to the table. That commitment extends beyond creating enterprise-grade smartphones, tablets and other mobile devices. It also encompasses the full scope of programs and partnerships that enterprise mobility initiatives entail.

Samsung has a compelling story to tell for each of the five mobile strategy steps described above.

Step 1. Mobility use cases and employee preferences

Samsung offers a broad portfolio of device form factors including smartphones, tablets, Chromebooks and laptop PCs. In addition to offering different screen sizes and formats, the Samsung devices support multiple operating systems, include premium and rugged models, and deliver an unmatched collection of features and functions. As a result, enterprises can find Samsung devices that match virtually any mobility use case.

When it comes to employee preferences, employees have already voted with their personal device purchases. As noted in the market figures cited earlier, Android-based devices dominate smartphone shipments, and Samsung dominates the Android smartphone sector with a nearly 40 percent market share. No other Android smartphone provider held more than a 6.5 percent market share in the second quarter of 2013, according to market research firm IDC.

Given these figures, companies with BYOD programs already have large numbers of Samsung devices active within their employee populations. Enterprises looking to update their mobile devices from earlier models that have fallen into disfavor should give appropriate weight to the mobile device choices their employees are making on their own.

Step 2: Industry-leading security and management capabilities

Samsung offers a broad suite of security and management capabilities. For example, the company's devices support Exchange ActiveSync (EAS), a protocol that helps mobile phone users be more productive by giving them secure access to their corporate email accounts, calendars, contacts and tasks. For security, the company provides a suite of advanced capabilities as part of the Samsung Mobile Security portfolio. Among these capabilities:

- **MDM support** – Samsung works closely with leading mobile device management providers to ensure that its portfolio of devices are compatible with, and optimized for, these critical management platforms. Samsung Mobile Security gives MDM systems the ability to exert fine-grained control over Samsung devices by providing access to more than 490 distinct IT policies that are exposed through more than 1,090 application programing interfaces.
- **Virtual Private Networks** – To give mobile professionals secure connections to corporate resources, Samsung's devices provide broad compatibility for many partner virtual private network (VPN) solutions and cover all levels of VPN security, including IPsec, PPTP and L2TP. Samsung is also the first company to provide Secure Sockets Layer (SSL) VPN for Android-based devices.
- **On Device Encryption (ODE)** – To protect data should a mobile device be lost or stolen, Samsung provides a high level of ODE for internal and external (SD card) memory. Samsung's ODE technology uses AES 256-bit encryption and is certified as compliant with the Federal Information Processing Standard (FIPS) 140-2.

CIO
Custom Solutions Group

Samsung has a large community of ISV partners that, collectively, offer more than 460 software solutions for Samsung's platforms. These applications include common mobile business offerings as well as a large number of industry-specific mobility solutions.

Complementing these capabilities is Samsung KNOX, a comprehensive mobile security solution for the company's smartphones and its other Android-based devices.

Samsung KNOX is designed to satisfy enterprise security requirements without compromising corporate security or employee privacy. In doing so, KNOX offers security for both platform and application.

KNOX platform and application security features include:

- **Trusted Boot**, the first line of defense against malicious attacks on KNOX-equipped devices, which ensures that only verified, authorized software can run on devices.
- KNOX also features **TrustZone-based Integrity Measurement Architecture** (TIMA), which runs in the secure world and provides continuous integrity monitoring of the Linux kernel to detect and notify when the integrity of the kernel or the boot loader is violated.
- In addition, KNOX offers **Security Enhancements for Android**, an enhanced mechanism that isolates applications and data in different domains to reduce threats from tampering with or bypassing application security, as well as from malicious or flawed applications.
- **Samsung KNOX Container** is a powerful solution for data leakage problems associated with the BYOD model. This KNOX application security feature safeguards enterprise data by creating a secure zone in the employee's device for corporate applications and encrypting enterprise data both at rest and in motion.

Step 3: Extensive apps and development tools portfolio

The worldwide popularity of Android-based devices has given rise to a huge collection of Android-compatible mobile apps. According to AppBrain, a website that tracks Android apps, there were nearly 875,000 Android apps on the market as of early November 2013.

In addition to being able to tap this massive pool of Android-compatible apps, Samsung works closely with many partners to develop or optimize apps specifically for Samsung's devices. As detailed below, Samsung has a large community of ISV partners that, collectively, offer more than 460 software solutions for Samsung's platforms. These applications include common mobile business offerings as well as a large number of industry-specific mobility solutions.

To support enterprise app development and customization needs, Samsung offers an Enterprise Software Developers Kit (SDK). Configured as an Android add-on, the Samsung Enterprise SDK allows qualified partners and customers to develop enterprise applications using the ODE, VPN, MDM and ActiveSync APIs its platforms provide.

With the Enterprise SDK, for example, developers can enforce "whitelisting" and "blacklisting" app policies. They can also monitor and control SMS usage and other costs; monitor, enable and disable on-device cameras, Wi-Fi and other device capabilities; and perform a variety of other enterprise-driven functions.

Step 4: Extensive partner ecosystem

Understanding that it couldn't meet all of the needs of enterprise customers on its own, Samsung has established a partner initiative called the Samsung Enterprise Alliance Program (SEAP). The program is administered by a Samsung enterprise business team made up of sales, marketing and R&D specialists. SEAP's more than 650 members include ISVs, systems integrators, value-added resellers and distributors; the program's membership is growing by about 15 percent each month.

SEAP is a tiered program, with members categorized as Platinum, Gold or Silver partners based on a variety of qualifications and capabilities. Among other factors, Samsung evaluates candidate partners based on their industry expertise, their size, their market coverage, their technological strength and their go-to-market capabilities.

The ISVs within the SEAP ecosystem include SAP, Cisco, Citrix and other major industry players, as well as a large number of industry-sector and mobility specialists. Among the offerings these partners provide are dozens of security, unified communications and collaboration solutions, as well as a broad collection of virtualization, messaging and business intelligence offerings. Samsung's ISV partners also offer a range of solutions designed for the needs of specific industry sectors including education, healthcare, finance, transportation and logistics, government, automotive, retail and hospitality, and aviation.

Step 5: Enterprise support and business continuity services

Samsung realized early on that the limited product warranties and support services available to individual mobile device consumers wouldn't cut it in the world of enterprise mobility. Corporations may require device support for several years, and they need support services to ensure the availability of these devices and the continuity of the business operations running across them.

To meet these needs, the company provides the Samsung Mobile Care Pack. As shown in Figure 2, this offering allows companies to mix and match a variety of warranty extension and servicing options across the entire portfolio of Samsung mobile devices.

Organizations can obtain Samsung Mobile Care Pack coverage for devices they purchase for their employees, as well as purchase extended warranties and service plans for personal devices that employees use as part of corporate BYOD programs.

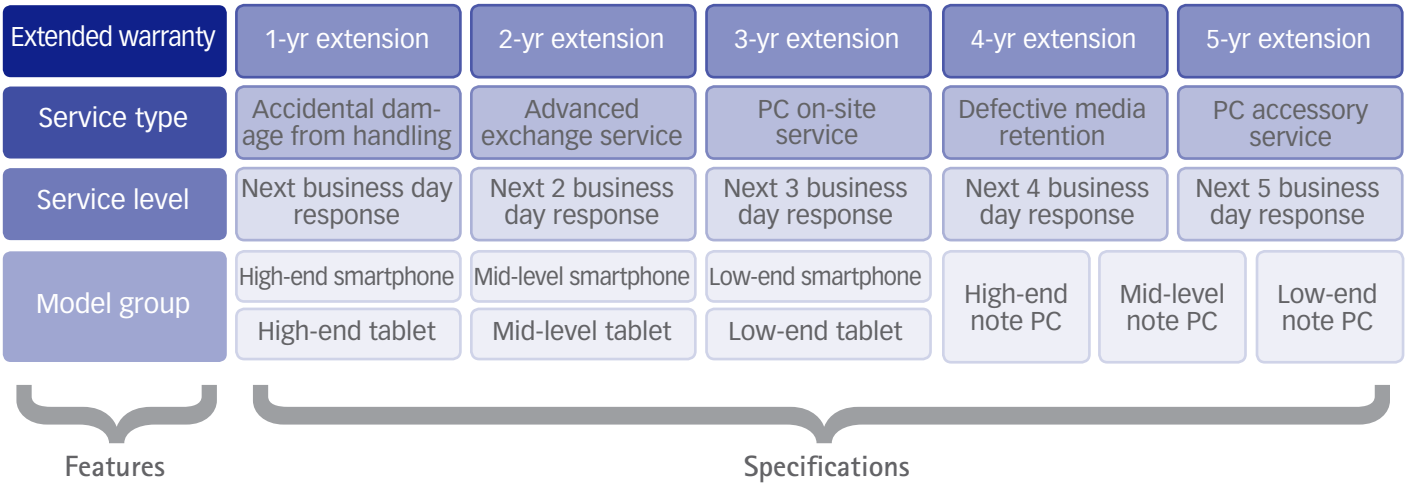
The Samsung Mobile Care Pack lets companies extend the basic device warranty by up to five years. It also offers an accidental damage-handling option to expand the limited warranty to include accidental damage from, for example, water, drops or electrical surges.

Mobile Care Pack customers can also take advantage of Advanced Exchange Services that provide replacement devices from a buffer stock to help employees stay productive rather than be idled while waiting for device repairs. In addition, they can tap Remote Care Services that provide remote problem diagnosis and repair by Samsung service representatives, eliminating the need for customers to go to a service center or wait for a services engineer to visit the site.

CIO
Custom Solutions Group

Figure 2. Samsung Mobile Care Pack provides selection of service options

SOURCE: Samsung



Partnering with Samsung to Meet Next-Generation Mobility Needs

Not much happens slowly in the world of high technology, and the mobility marketplace is among the most active and fast-evolving of technology sectors. The presence of hundreds of millions of advanced smartphones, tablets and other mobile devices across the business landscape has dramatically altered the enterprise status quo.

Companies hoping to stay competitive and wanting to achieve maximum operational efficiencies must keep pace with the evolving capabilities – and shifting fortunes – of different mobile devices. To best accomplish this goal, they must consider not only the capabilities of the devices themselves, but also a host of other factors critical to the overall success of enterprise mobility programs.

If they conduct these assessments and evaluations in a comprehensive fashion, enterprises are likely to find Samsung emerging as an obvious mobility partner. The company's portfolio of mobile devices is arguably the most powerful and popular available from any vendor today. In tandem with its device innovation, Samsung has created a wide range of technologies and programs designed to meet the demanding requirements of its enterprise customers.

The breadth of its device portfolio, the sophistication of its technology and the range of its business-focused partnerships and programs have already established Samsung as a leading player in the enterprise mobility scene. Based on its commitment to this demanding customer base, Samsung is likely to hold this leadership position for many years to come.

About Samsung Electronics Co., Ltd.

Samsung Electronics Co., Ltd. is a global leader in technology, opening new possibilities for people everywhere. Through relentless innovation and discovery, we are transforming the worlds of televisions, smartphones, personal computers, printers, cameras, home appliances, LTE systems, medical devices, semiconductors and LED solutions. We employ 236,000 people across 79 countries with annual sales exceeding KRW 201 trillion.

For more information

To discover more, please visit
www.samsung.com

For more information about Samsung Enterprise Mobility, visit us online at:
www.samsung.com/enterprise

For Samsung Enterprise Alliance Program, visit:
www.samsungmobileb2b.com