WHITE PAPER

Successfully Embracing Mobility in the Enterprise

Balancing Act: Open Yet Controlled

Enterprises everywhere are caught up in the mobile computing revolution. Powerful smartphones and tablets with broadband wireless connections enable employees at all levels to be productive — to access data and get work done — whenever they want, wherever they happen to be. Further, workers increasingly expect to bring their own mobile devices to work. The onus then falls to IT to strike a balance, connecting them to corporate data resources securely while keeping personal information and corporate data separate.

It's a tall order. To succeed, CIOs must make sure that their IT groups are armed with mobile security and mobile device management (MDM) tools to establish and enforce corporate data policies across the mobile workforce without sacrificing usability.

CIOs realize that mobility in general, and the bring-your-own-device (BYOD) trend in particular, are turning IT's traditional approach to PC provisioning, management and security on its ear. Instead of a structured, top-down approach to device configuration and assignment in a network environment supporting only one or two operating systems (OSes), IT faces droves of small, untethered devices that might be running any of a half dozen mobile OSes. Most IT staffs can't be fluent in them all, so a different approach to provisioning, management, security and support is in order.

Specific BYOD Challenges for CIOs

To conquer the mobility conundrum, there are a few key decisions to make and actions to take.

CIO
Custom Solutions Group

SAMSUNG

» Which Mobility Model?

The first decision is which mobility model to support: Fully corporate-liable, fully employee-liable (BYOD) or a hybrid of both. CIOs should engage other departments and business units in making this decision.

- **FULLY CORPORATE-LIABLE.** The enterprise procures, manages and secures all end-user devices, paying monthly fees. This model is the opposite of BYOD.
- **FULLY EMPLOYEE-LIABLE (BYOD).** Employees purchase personal devices and want to use them at work. Enterprises need to identify, secure and manage them.
- **HYBRID.** A mix of corporate- and employee-liable devices. Enterprises can use new mobile security and management tools to implement top-down control regardless of who bought the device.

» Establish a Guide for Mobile Behavior

Whichever model is chosen, CIOs need to establish policies for appropriate access and user behavior. These policies must be written clearly and shared with employees. They will be based on the organization's corporate policies and risk profile and any regulatory compliance policies that apply. By coordinating with the appropriate departments or by instituting a mobility group within the IT department, CIOs can determine access policies for each device type and employee profile. There might be certain devices, for example, to which you automatically deny access because they emit large volumes of pings and alerts that degrade your wireless LAN (WLAN) performance.

Once corporate access decisions have been made and documented, the organization can look to mobility management and security tools to automate processes and enforce policies.

» Automate Policy Setting and Enforcement

Once you have a broad policy for the devices, you can use automated mobile security and management tools to classify employees into separate user groups based on their access rights. These classifications might match existing VLANs or other user groups that your enterprise already has set up. Then you can assign policies to each user class. For example, you might want to encrypt all data stored on certain users' mobile devices and SD cards. You might want to specifically enable or disable functions such as cameras, Bluetooth connections and Short Message Service (SMS), depending on the user's role and risk level.

From an expense management perspective, you might want dual-mode devices to default to "free" Wi-Fi services, where available, to save on cellular costs. You might want to disable international roaming for certain users or alert them when they cross a border and start incurring extra fees.

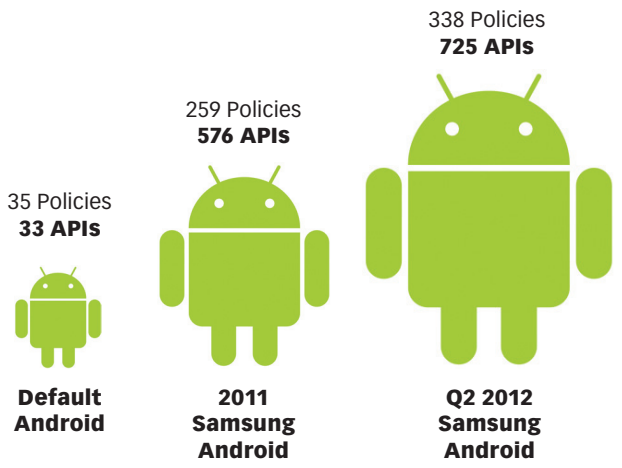
Mobile Security Solution Considerations

Mobile security and management are maturing disciplines. Many approaches require installing a security solution (hardware, software or virtual) on premises. Some providers also offer a cloud/software-as-a-service (SaaS) version of their solution. Regardless of the model you choose, client software is installed onto users' devices. You'll need a cooperative arrangement with employees using their own personal devices to load the agent onto those devices.

There are certain key capabilities that should be in any mobile security and management tools you choose:

- **MOBILE DEVICE MANAGEMENT (MDM).** A system for enabling your IT department to remotely configure, monitor, control and administer all deployed mobile devices. MDM systems vary widely in the capabilities they support. For example, among the features they might offer are any or all of the following: inventory monitoring; hardware/software component management; application provisioning and management; network access control; help desk features; location-based services, such as remotely locating missing devices and wiping data on them; security management; expense management, and other innovative functions. Comprehensiveness of features is important in an MDM system, because it is difficult and expensive to install and manage multiple systems that each solve just a piece or two of the mobility management puzzle.
- **VIRTUAL PRIVATE NETWORK (VPN).** An encrypted tunnel through shared networks such as the public Internet and mobile broadband (3G/4G) networks that provides secure corporate network access to mobile and remote employees. VPNs "scramble" data in transit so unauthorized users intercepting it can't read it. There are a number of different types of VPNs. Most common:
  - **Secure Sockets Layer/Transport Layer Security (SSL/TLS) VPNs.** These allow users to securely access multiple back-end network applications and services through a Web browser on their mobile device.
  - **IPsec VPNs.** IPsec VPNs grant or deny access to the corporate network as a whole, based on information at the network (routing/IP) layer, rather than on an application-by-application basis like SSL VPNs do.
- **ON-DEVICE ENCRYPTION (ODE).** The ability to encrypt data residing on users' devices so that it can't be read by anyone other than the authorized user. ODE protects any local data such as customer information, confidential corporate information and contacts. Encryption can take place in two places, depending on policy:
  - **Data stored in the device's internal memory**
  - **Data stored on external SD cards**

FIGURE 1: Progress with Android Enterprise Policies



Samsung GALAXY Android Platform: Enterprise-Ready

Despite Android's immense success in the consumer market, IT decision makers have been reluctant to embrace it. That's because the basic platform originally lacked enterprise-class security and application compatibility attributes. Samsung is the market-leading Android device supplier: according to Strategy Analytics, more Samsung Android handsets shipped in the first quarter of 2012 than any other, regardless of mobile OS, accounting for 25.4% of mobile subscribers[1]. As the Android leader, Samsung has taken it upon itself to make sure its Android implementation meets IT expectations.

For its GALAXY phones and tablets, Samsung has built a set of policies that go far beyond the basic set created by Google for Android. By partnering with industry-leading vendors who use Samsung Enterprise SDK application programming interfaces (APIs) to build the added functionality into their security and MDM products, Samsung has taken a holistic approach, combining best-of-breed features into a common, integrated platform.

» Case In Point: SAP Standardizes on Samsung for Android

When Samsung released its enterprise APIs, Oliver Bussmann, CIO of SAP AG, standardized on Samsung GALAXY Android for its employees and also became a Samsung partner.

"We are very pleased to offer Samsung devices to our global workforce as part of our internal device-agnostic strategy," says Bussmann. "It's important for our employees and also our customers to have choices, and SAP software running on Samsung's Android devices will allow our workforce to do business in the moment. Furthermore, it's critical that we can secure our business data on these devices using an extensive range of IT policies with enhanced security and manageability features closely integrated with SAP Afaria MDM."

» Samsung GALAXY Enterprise-Class Specifics

- **SECURITY.** Samsung has reinforced the GALAXY Android platform with capabilities to protect against damaging security breaches. Several of them are highlighted below.
  - » **MDM.** With 338 IT policies through 725 APIs (see Figure 1), Samsung enables companies to enhance software and hardware component control and prevent mobile security failures. Samsung provides broad compatibility with prominent MDM partner solutions with a comprehensive set of features:
    - **Remote configuration.** Over-the-air secure configuration distribution of Exchange ActiveSync, Cisco AnyConnect, IMAP and POP3 email, Wi-Fi, Access Point Name (APN), Web proxy and other settings.
    - **Inventory monitoring.** Visibility into details about the device, such as total memory usage, installed application list and OS version.
    - **Application management.** Ability to install and remove apps, disable and enable apps and enforce IT policy about which applications must be deployed ("whitelisting") and which should be blocked ("blacklisting").
    - **HW/SW Component management.** Enablement and disablement of on-device cameras, as well as Bluetooth, Wi-Fi and USB connections. IT can also reset devices to original "factory" settings, upgrade OSes, manage Google backups and enable mobile-to-PC syncing via a feature called Samsung Kies.
    - **Help Desk.** Ability to support staff at multiple locations from one central help desk.
    - **Location-based service.** Discover location of missing devices and either enforce territorial boundaries and policies associated with that device or wipe the device to remove confidential data.
    - **Kiosk mode.** Ability to simplify the user interface by presenting only the required applications, disabling hardware keys such as "power off" and removing the notification bar.
    - **Security management.** Ability to provision security policies such as password settings and data encryption on/off and to install and expire certificates and firewall settings.
    - **Expense management.** Visibility into cost-related information like call and SMS usage levels and call duration times. IT also has the ability to disable data roaming and tethering and limit the number of SMS messages users can send, all to provide real-time cost control.
  - » **FIPS–140–2 Certified Data Encryption.** The native Android OS supports 128-bit Advanced Encryption Standard (AES) encryption for internal memory in Android devices. By contrast, Samsung has enhanced its Galaxy on-device encryption support using the more secure AES 256-bit data encryption algorithm and also extends AES 256 to external SD cards for still higher levels of security than other devices.

[1] http://www.strategyanalytics.com/default.aspx?mod=pressreleaseviewer&a0=5211

Samsung's encryption technology is FIPS-140-2 certified to protect against data break-ins. FIPS-140-2 is a security requirement mandated by the Federal Information Security Management Act of 2002 (FISMA); supporting it enables Android devices to be used in government agencies to access unclassified information. The standard also requires features that show evidence of tampering, so enterprises can see if a device has been "rooted" and filter the device off the network.

» **VPN Support.** Samsung was the first Android platform to support SSL/TLS VPNs through its integration partners Cisco, F5 and Juniper Networks, allowing enterprises to select the VPN of their choice. Samsung GALAXY provides broad VPN compatibility for most partner VPN solutions and covers all levels of VPN security, including support for SSL and IPsec, as well as Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Tunneling Protocol (L2TP) VPNs.

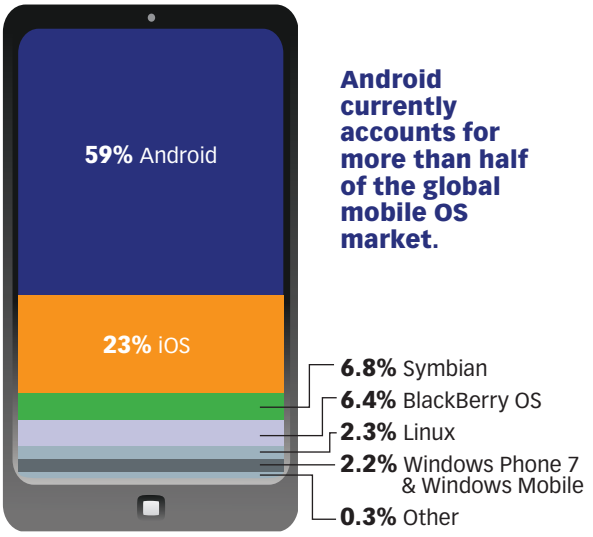
- **EXCHANGE ACTIVESYNC (EAS) ENHANCEMENTS.** Most Android devices support Microsoft's Exchange ActiveSync protocol; however, Samsung GALAXY devices have enhanced this support to offer the most comprehensive EAS implementation in the industry (see Figure 2). Samsung has integrated with EAS servers and extends EAS policies to Samsung GALAXY Android devices at no extra cost.

The Samsung GALAXY implementation was the first to support S/MIME encrypted messages in EAS. The platform also supports Lightweight Directory Access Protocol (LDAP) so that enterprise users can sync with the corporate address book and access their email systems from anywhere — and do so according to existing corporate access policies.

FIGURE 2: Exchange ActiveSync (EAS) Support Comparison

Standard Android™ Features	Additional Samsung Features
✔ Direct Push	✔ Server Search
✔ Email/Calendar/ Contact Sync	✔ Out of Office
✔ Remote Wipe	✔ Follow-Up Flags
✔ Sync Multiple Folders	✔ Set High Importance Status
✔ GAL Lookup	✔ Partial Download
✔ HTML Email View	✔ Re-Sync™ All Data from Server to Phone
✔ Auto Discover	✔ Conversation View
✔ Meeting Request — Accept/Reject	✔ OCS/Lync Voicemails in Inbox
	✔ Free/Busy Lookup
	✔ Reply/Forward Status

FIGURE 3: Worldwide Mobile OS Market Share, Q1 2012



Android currently accounts for more than half of the global mobile OS market.

Source: IDC Worldwide Mobile Phone Tracker, May 2012

Taming the Anarchy

Mobility has completely disrupted traditional approaches to provisioning, managing and securing end-user computing devices in enterprises. Enterprises need to take a structured approach to mobility that identifies classes of users and device types, then create policies for how to treat the different user groups, devices and applications as they attempt to connect to the network.

In this spirit, Samsung is making the open Android platform enterprise-ready. A comprehensive portfolio of policies and APIs are already at work to secure and manage Samsung Android GALAXY devices at levels that fall into the comfort zone of corporate IT departments.

Samsung makes it possible for IT organizations to establish and enforce corporate data policies across the mobile workforce without sacrificing usability. One way is through partnership with leading VPN and MDM vendors. Another is by enabling comprehensive Android GALAXY integration with Microsoft EAS so that user interactions with calendars, contact lists and unified communications features appear seamless.

With Android phone and tablet usage steadily increasing (see Figure 3), savvy CIOs can now deploy them with the enterprise-class security, management and usability to which they have long been accustomed. ■

For more information, visit
www.samsung.com/enterprise