Mobile Device Management

BYOD to the Enterprise

making IT happen

When it comes to choosing our next smartphone or tablet for personal use, we are spoilt for choice because of the wide range of devices on the consumer market - both in terms of functionality as well as design and look.

Yet when it comes to accessing applications for work, people are often stuck with a limited number of antiquated models that the company has approved for use - because only those models have been audited for security and compatibility to the company's enterprise IT systems.

As a result, it is not an uncommon sight to see people carrying two smartphones - a spanking new model for personal use, and a separate out-dated one specially for accessing the company's applications while on the move. It would be just ideal, if there is an increased adoption of the Bring-Your-Own-Device (BYOD) concept to the enterprise, enabling the individuals and unleashing their productivity.

A New Computing Landscape

Enterprises need to be prepared for the influx of mobile devices into the enterprise space. Traditionally, the focus of enterprise IT has been on securing networks, servers and desktops. Prior to allowing a new device or model to tap into the company's IT systems, a thorough and time-consuming audit process is usually carried out to check on security and compatibility. To keep up with the fast paced consumer world, and to enable employees, partners and customers to access the company's mobile applications using the latest devices on the market, a more responsive approach towards mobile device management is needed.

The strategy for Enterprise Mobility would need to embrace a multi-vendor and multi-platform environment, to have a viable management infrastructure to control access, enforce policy, ensure security and safeguard corporate data and networks.

CONSIDERATIONS

- Scalability and the ability to support and manage the explosive growth of mobile devices and mobile applications, as well as compliance to the corporate IT policies
- Security - Although mobile devices increase the productivity of the organisation and employees, their mobile nature presents a clear risk to the security of the corporate network
- High costs to provision for supporting mobile devices from the plethora of vendors and platforms

SOLUTIONS

- Platform: Deploy a platform that ensures mobility is managed holistically, from a single console with a standard set of management tools and policies
- Security: Protect the enterprise's proprietary information with security features such as authentication, encryption, lock & wipe, and data fading

BENEFITS

- Enterprises can remotely provision for both corporate and personal mobile devices through an approved and responsive enrollment process
- Protect sensitive data with effective and secure management of mobile applications
- Gain visibility and control of the mobile devices in the entire enterprise workspace, with pervasive information of the software and hardware inventory

Moving Towards the Unwired Enterprise

The acceptance of individual-liable devices in the enterprise workspace is powering the concept of the "Unwired Enterprise". This will enable the seamless transfer of corporate information from the data center to any device, bringing the information to the point of action - be it within the premises of the company or while the user is out of the office and on the road.

All these changes in the computing landscape require a strong Mobile Device Management policy and management solution to both enable these consumer devices as well as enforce the security policies. The Mobile Device Management (MDM) solution should allow the management of mobile devices across platforms and vendors supporting the entire device lifecycle, from provisioning to decommissioning.

Explosion of Mobile Applications and Productivity Applications

The growing complexity of mobile software, both enterprise and personal, is here to stay. Users can easily download any number of applications from the Web or from the AppStores for their devices.

These applications may contain malware that can put sensitive corporate information at risk and render the device non-compliant to corporate baselines. Downloading a large number of applications can also slow down the device and max out the storage on the device, such that the user is unable to install additional corporate applications that are needed.

For corporate-liable devices, the IT department can enforce whitelist and blacklist applications so that the end users can download only those applications on the approved list. For individual-liable devices, IT department should be able to manage the corporate applications alone without interfering with the rest of the applications.

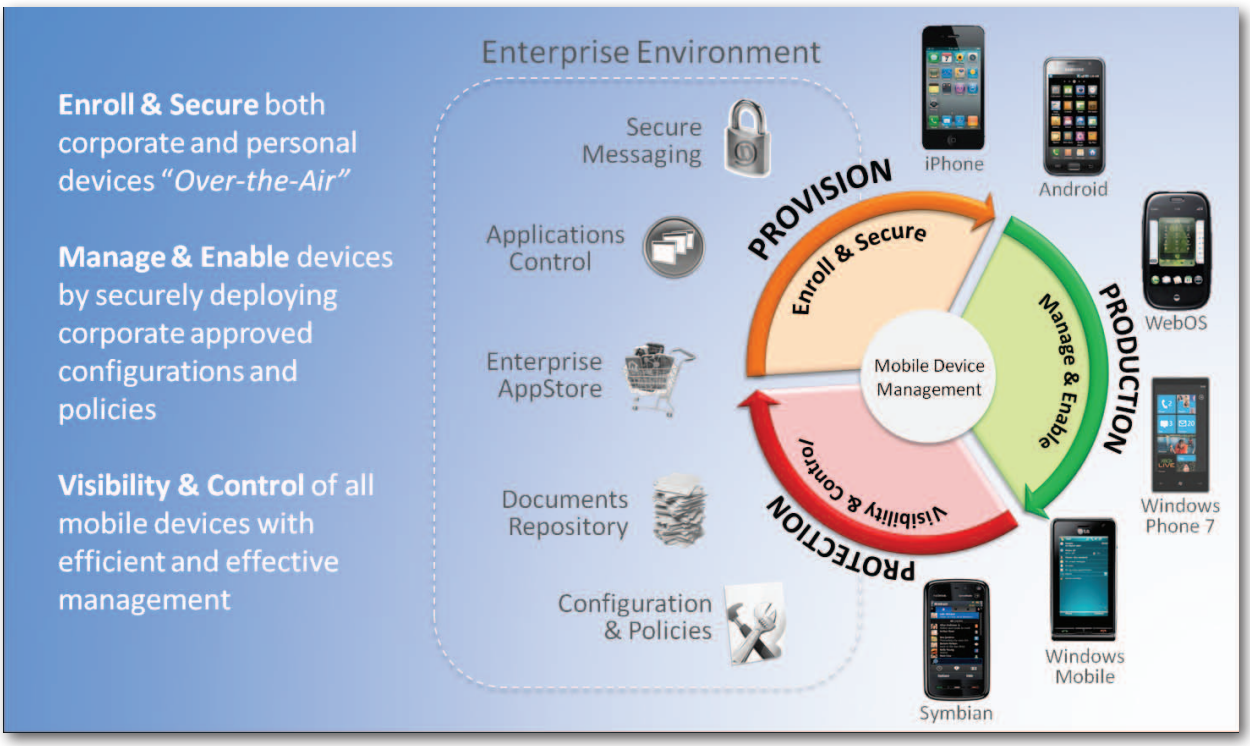
Implementing an MDM Solution for the Enterprise

An MDM strategy should be developed as part of the overall IT strategy for the company. This is critical in order to successfully balance enterprise security with user privacy on user-owned devices. The strategy should cover the scalability and ability to support and manage the explosive growth of mobile devices and mobile applications, as well as compliance to the corporate IT policies.

NCS comprehensive suite of MDM solutions help enterprises to establish a viable and secure enterprise mobility environment:

- A shared Management Infrastructure to centrally deliver services to subscribed customers based on a multi-tenanted model
- A one-stop Operations Centre for remote management and support
- Bundling of Software and Services as a subscription-based Per Device offering
- Portal-based to provide maximum self-service facilities to the customers
- Independent of network, handset, OS & application for services delivery

For more information, email cps@ncs.com.sg



ncs making IT happen
NCS Pte. Ltd.
5 Ang Mo Kio Street 62, NCS Hub, Singapore 569141 T: 65. 6556 8000 F: 65. 6556 7000
E: reachus@ncs.com.sg Website: www.ncs.com.sg
A member of the SingTel Group