



Integrated Mobility Management™

Whitepaper Series

**Paper 2 – Protecting All Borders in the
Mobile Enterprise**

Integrated Mobility Management™ refers to IT systems and processes provided by a business partner to help enterprises plan, procure, provision, activate, manage and support mobile devices, network services, management systems, mobile applications and application stores. As large enterprises have come to depend more and more on 'mobility' as a means of conducting business, the business case has grown stronger for them to outsource the management of these mobility systems to a professional partner. Outsourced managed services allow enterprises to take advantage of economies of scale and operation. This allows the enterprise to focus more tightly on strategic functions, and as a result, create more value for the business. Sometimes referred to as 'managed mobility', the research firm Gartner currently breaks 'managed mobility' into six categories:

- Sourcing and logistics management
- Mobile service management
- Device and system management
- Application and collaboration management
- Security and content management
- Program and financial management

In this whitepaper we specifically discuss the security solution requirements of a professional managed mobility offering, and in particular the need for a holistic mobile security management solution approach.

Challenges of Securing Mobile Devices

Mobile computing devices and the BYOD phenomenon introduce risk, especially the risk of data loss, unauthorized use and malware propagation. Mobile Device Management (MDM) systems are great tools for enterprises that wish to better manage the plethora of smartphones and tablets that are being used in corporate environments. Most MDM systems can also help IT security managers secure the sensitive corporate data that is frequently stored on such devices. However, MDM systems by themselves do not address the following challenges:

- 1) MDM systems can only see devices that have already been enrolled in the system. This leaves IT managers blind to unmanaged devices on the network. MDM systems are not designed to control access to the network. IT security managers need a way to prevent unauthorized devices on the network, and prevent infected, compromised or jail broken devices from attacking the network.
- 2) MDM systems are often operated as a separate IT management silo by a group other than IT security. The MDM system typically has a separate set of management screens, policies and reports. This presents a challenge for IT security managers who want a unified set of policies for access control, compliance monitoring and reporting across network tiers and types of endpoint devices.

Similarly, Network Access Control (NAC) is commonly used to control access to enterprise networks. This helps prevent data loss by ensuring that unsecured, unmanaged devices do not have access to corporate data on the network. However, if your goal is to push corporate data onto mobile devices, NAC by itself is an insufficient security control. You also need to protect the data on the device itself with controls provided by MDM.

No matter where your organization is on the mobile adoption spectrum — blocking, tolerating, supporting or promoting the use of mobile devices for business use — you need a way to enforce security policy. You need real-time visibility and control over your network and the mobile devices.

Typically, MDM vendors over-emphasize the value of their MDM solution, and NAC vendors over-emphasize the value of their NAC solution. One of the values of an Integrated Mobility Management partner is their ability to recommend and implement a holistic solution that covers all the security bases.

Holistic mobile security management solutions

One of the clear thought leaders in the mobile security space is ForeScout Technologies, headquartered in the U.S. Although their pedigree is mainly in the NAC space, they offer a nicely integrated solution that combines their market leading NAC system with a third party MDM system. This integration lets enterprises manage their MDM solution within the broader context of unified security control. ForeScout's MDM Integration Module provides MDM systems with enhanced security and unified network access policy management for corporate and personal mobile devices on the enterprise network. The MDM Integration Module works with ForeScout's network access control (NAC) platform, ForeScout CounterACT™, and your MDM system to provide real-time visibility and control of devices on your network — wired and wireless, managed and unmanaged, PCs and handheld devices. Currently, ForeScout supports the following MDM systems: AirWatch, Citrix XenMobile, IBM MaaS360, MobileIron, SAP Afaria.

In our view, the benefits of combining NAC with MDM are clear:

- 1) The MDM system helps you manage and control personal devices. In this way, you can maintain strong security by ensuring that passwords are appropriately set, the mobile devices are not jailbroken, data can be wiped from the device when needed, etc..
- 2) The NAC system helps you manage and control the network. In this way, you can ensure that only certain types of devices are allowed onto the network, and only if they have already been enrolled into your MDM system and assessed to be compliant with your mobile security policies.
- 3) The NAC system can help your employees on-board new mobile devices quickly and easily. Immediately after an employee brings a new mobile device into the office, the

NAC system detects that device, determines whether it has already been enrolled into your MDM system, determines whether it should be enrolled into your MDM system (based on who the owner is and what type of device it is), and then automatically sends the mobile user to the MDM system enrolment portal. This automation reduces the number of help desk calls and helps your employees get their devices up and running faster.

- 4) The NAC system allows you to limit where mobile devices can go on your network. This is especially important for BYOD devices including traditional computers running Windows or Mac operating systems. Typically, BYOD devices are not as fully secured or trusted as fully managed computers owned by the company, and thus some degree of network control is appropriate.
- 5) The NAC system can function as your single pane of glass where you can see and report on the status of all devices in your organization – PCs, Macs, Linux, as well as the plethora of mobile devices that your employees are using.

Enterprise mobility demands an integrated, end-to-end approach, co-ordinated across all areas of security (MDM, NAC) and spanning everything from device procurement policies to overall programme governance.

Bluewater™ Integrated Mobility Management™, from Telestar™, is one such solution. Bluewater™ procures, secures, controls, assists and governs all aspects of the mobile enterprise. In the critical area of security, Bluewater™ relies on ForeScout CounterACT™ integrated with MDM to secure the borders of your mobile enterprise.

Mobility has brought enterprise computing into a new world of flexibility, but also of security risks. To look to address mobile security with MDM only is to look only one small part of the challenge. Securing all the borders of the mobile enterprise, especially in a BYOD world, demands an integrated security solution.

About Telestar

Telestar Communications is an ICT consultancy business that provides Corporate, Enterprise and Government businesses and agencies with a single point of accountability across all their telecommunications and information technology needs.

Telestar provides Bluewater™ Integrated Mobility Management™, managing mobility operations for large enterprises and governments across the East Asia and Pacific region.