# Addressing the mobility gap in corporate security

By Fred Mitchell

16 Jan 2015

Mobility and Bring Your Own Device (BYOD) are some of the fastest growing trends, both locally and across the globe. From laptops and notebooks to ultrabooks, smartphones and tablets, the sheer number of mobile devices available today is driving the requirement for networks to open their borders, potentially creating significant holes in the fabric of corporate security.

Image: www.freedigitalphotos.net

In addition, mobile devices are increasingly used to access business-related and potentially critical data, resulting in this data frequently being stored on unsecured, highly portable devices that are prone to loss and/or theft. Closing the mobility gap within security requires a multi-faceted approach, including policy, process and tools.

Mobile devices have the potential to open up corporate networks to a wide variety of threats, and tackling this challenge requires a comprehensive mobility strategy with all-encompassing security as the main focus. Perhaps the most well understood aspect of mobile security is the need to protect against malware and other cyber threats. Mobile threat management is increasingly important for all users of mobile devices, particularly the corporate environment where BYOD exposes sensitive information to vulnerabilities. However, this is just one aspect of a full mobile security strategy, which should also incorporate Mobile Application Management (MAM) as well as Mobile Device Management (MDM).

Application management is an essential component of mobile security, as BYOD introduces the potential for employees to utilise unapproved mobile or cloud-based applications (apps), which in turn creates the potential for corporate data to be leaked. Attackers are also increasingly targeting mobile devices with malware introduced through unauthorised apps. Targeted application management goes beyond traditional device management to deliver additional flexibility and control while still empowering the mobile enterprise.

MDM is another essential component, as organisations must remotely manage smart devices, including resetting or blocking these devices should they be lost or stolen. Software delivery, application repair, inventory, file encryption and more are all important components in ensuring mobile security. In addition, mobile devices need to be incorporated into

Disaster Recovery (DR) strategies and solutions, to ensure business continuity is not compromised as a result of lost data on a mobile device.

As BYOD essentially allows users to make use of their personal devices irrespective of brand or platform, mobile security should provide heterogeneous device support and comprehensive visibility and control over all different Operating Systems (OS). Security and policy controls, including backup, passwords, remote wipe, application restrictions and so on, are also essential. Corporate and personal data should be separated, to limit privacy concerns and optimise enterprise backup and recovery. In addition, email, enterprise applications and corporate content need to be incorporated as part of mobile management in order to meet DR objectives.

Comprehensive mobile security and management requires protection at all layers, including the device, application and data. IT needs to apply consistent levels of security, with one standard and strategy applicable whether employees use corporate-owned or BYOD devices. In order to protect the enterprise, as well as employee privacy, mobile security must ensure that corporate data is isolated and protected from data leakage, malware and unauthorised access.

As the range and variety of mobile devices is constantly growing and changing, mobile security furthermore needs to be flexible enough to grow and change with the evolving needs of the enterprise. Above all, security needs to remain invisible to users, in order to ensure optimal employee productivity and satisfaction.

Mobility is the future, and enabling employees to have their choice of device is essential in catering to an increasingly informed and consumerised workforce. However, such trends require a re-evaluation of security practices and procedures. Sacrificing security for the sake of mobility is not a long-term solution, and will only invite trouble down the line. Ensuring a comprehensive mobile security strategy, with MDM, MAM, mobile threat management and a variety of other facets is essential in securing enterprises while leveraging the productivity and efficiency advantages of the mobile workforce.

## ABOUT THE AUTHOR

Fred Mitchell is Software Division Manager at Drive Control Corporation