Security still the key in delivering mobility

By Anthony Doherty   30 Apr 2015

In the mobile-first, cloud-first era, two trends are powering the wave of mobility sweeping across the enterprise. The first of these is 'Bring your own device' (BYOD) whereby personnel-owned mobile devices are used for work, while the second trend is the increasing usage of Software as a Service (SaaS).

Anthony Doherty

This means that enterprise mobility now has to incorporate data protection at device, app, and data level through technologies such as 'rights management'. For this to happen, businesses have to shift their security approach from a traditional device management approach to a user-centric one.

User-focussed device management for the digital era

Shifting the approach to user-centric begins with rights management, because of the potential risk of data loss associated with BYOD and enterprise mobility. Rights management involves the encryption of files and, then, managing access to those files based upon rights related to an individual's active directory credentials.

With Enterprise Mobility Suite (EMS), Microsoft's rights management is built right into the EMS solution in the form of Azure Rights Management, a simple solution for enterprises operating within compliance-based industries.

For example, construction firm Walsh Group required an enterprise mobility solution to accommodate the proliferation of employee-owned devices used on job sites across the US. The company adopted EMS to drive and manage its BYOD strategy, and consequently has experienced improved security, enhanced collaboration that promotes business agility, as well as improved information flow, which helped the business win contracts.

Managing devices, apps, and identities

Identity and access management allows the IT department to centrally manage identities across the data centre and the cloud, providing secure single sign-on to all applications. Having identity management built right into EMS by way of Azure Activity Directory enables the solution to keep pace with the growth of BYOD and increased usage of SaaS applications within the enterprise.

Microsoft's EMS solution helps minimise the complexity involved with keeping BYOD items secure along with the corporate data accessed. It offers mobile device management and mobile application management in the cloud or on premises, all from a single console through Microsoft Intune.

Today, many more employees want to use their mobile devices to access and share corporate resources anywhere, anytime. Enterprise mobility provides this agility for staff to communicate and collaborate more effectively on projects.

EMS unifies identity, data, and mobile device management in a user-centric approach, enabling employees to be more productive by having the freedom to work from anywhere on virtually any device with full, highly secure access that IT can monitor and manage easily and effectively.

ABOUT THE AUTHOR

Anthony Doherty is Windows Business Group Lead of Mcrosoft.