Enterprise Mobility Management

Making sure the fundamentals are right

Introduction

Mobility and bring-your-own device (BYOD) are transforming the way people work and the way businesses support them. At Wanstor we believe there is more to mobility than simply enabling remote access. To unlock the full potential of enterprise mobility, IT departments need to allow people the freedom to access all their apps and data from any device, seamlessly and conveniently.

Mobile devices also call for the right approach to IT security to protect business information as they are used in more places, over untrusted networks, with a significant potential for loss or theft. The IT department has to maintain compliance and protect sensitive information wherever and however it's used and stored, even when business and personal apps live side-by-side on the same device.

In this article Wanstor's Mobility experts have developed a set of key points which the IT department need to take notice of as an enterprise mobility strategy is developed.

Protect and manage key assets, data and information

As employees access data and apps on multiple devices (including personally-owned smartphones and tablets) it can no longer be seen as realistic for IT to control and manage every aspect of the environment. At Wanstor we believe the approach IT teams should take is to focus on what matters most for a business across devices, data and information then choose the right mobility management models that make the most sense for your business and your mobile use cases.

Generally it is accepted there are four models to choose from, either individually or in combination. Mobile device management (MDM), Mobile hypervisors and containers, Mobile application management (MAM) and Application and desktop virtualization. Choosing the right mix of these 4 models will be intrinsically linked to your businesses success.

User experience needs to be at the centre of your thinking

Mobile devices have been a key driver of consumerization in the enterprise, giving people powerful new ways to work with apps and information in their personal lives. This has raised the expectations around IT and the services they provide particularly around mobile devices.

No longer can IT teams put strict controls on users instead they must offer an IT experience that compares with the freedom and convenience allowed by consumer technology companies. At Wanstor we always suggest before MDM planning gets underway that the IT team sits down with a range of users and talk about their needs and preferences to make sure the mobility strategy which is going to be put in place gives them what they really want.

> It can no longer be seen as realistic for IT to control and manage absolutely every aspect of the IT environment

As the IT team works to deliver a superior user experience, Wanstor experts suggest that they examine ways to give people more than they expect and provide useful capabilities they might not have thought of e.g.

- Allow employees to access their apps and data on any device they use, complete with personal settings, so they can start work immediately once they have been given their work device
- Give people the choice of self-service provisioning for any app they need through an enterprise app store with single sign-on
- Automate controls on data sharing and management, such as the ability to copy data between applications, so people don't have to remember specific policies
- Define allowed device functionality on an app-by-app basis, so people can still use functions such as printing, camera and local data storage on some of their apps even if IT needs to turn them off for other apps
- Make it simple for people to share and sync files from any device, and to share files with external parties simply by sending a link.

By developing a mobility strategy alongside the collaboration of users, IT teams can better meet users' needs while gaining a valuable opportunity to set expectations. This helps to make sure employees understand IT's own requirements to ensure compliance.

Avoid bypassing

Bypassing company controls and policies via a mobile device represents the worst-case scenario for enterprise mobility. It is surprisingly common that many users if they cannot find/access what they want in terms of IT on their mobile device will bypass IT altogether and access their own cloud services, apps and data.

Many people think great employees are accessing what they want, when they need it. Actually nothing could be further from the truth. Employees accessing unknown apps, sensitive data via public clouds and downloading files which bypass the visibility and control policies of IT mean a business is extremely vulnerable to attack. In reality IT policies and user education can only go so far to prevent bypasses from happening, realistically, if it’s the best solution for someone’s needs and it seems unlikely that IT will find out, it’s going to happen. This makes it essential to provide people with an incentive to work with IT and use its infrastructure, especially when it comes to sensitive data and apps. The best incentive is a superior user experience, delivered proactively and designed to meet peoples’ needs better than the unmanaged alternative.

Embed mobility in your service delivery strategy

Mobile users rely on a variety of application types-not just custom mobile apps, but also third party native mobile apps, Windows apps and SaaS solutions. In developing a mobility strategy, IT teams should think about the mix of apps used by the people and groups in their business, and how they should be accessed on mobile devices. It is widely accepted that there are four ways for people to access apps on mobile devices: Native, Virtualized access experience, Containerized experience and through a fully managed enterprise experience.

For most businesses, a combination of virtualized access and a containerized experience will support the full range of apps and use cases people rely on. This also makes it possible for IT to maintain visibility and control while providing a superior user experience. People can access hosted applications and native mobile apps - as well as SaaS apps such as Salesforce and NetSuite - through a unified enterprise single sign-on. When an employee leaves the business, IT can immediately disable the person’s account to remove access to all native mobile, hosted and SaaS apps used on the device.

Define networking requirements

Different applications and use cases can have different networking requirements, from an intranet or Microsoft SharePoint site, to an external partner's portal, to a sensitive app requiring mutual SSL authentication. Enforcing the highest security settings at the device level degrades the user experience unnecessarily; on the other hand, requiring people to apply different settings for each app can be even more tiresome for them.

By locking down networks to specific containers or apps, with separate settings defined for each, the IT team can make networking specific to each app without requiring extra steps from the user. People can just click on an app and get to work, while tasks such as signing in, accepting certificates or opening an app-specific VPN launch automatically by policy in the background.

Protect sensitive data

Unfortunately in many businesses, IT doesn't know where the most sensitive data resides, and so must treat all data with the same top level of protection, an inefficient and costly approach. Mobility provides an opportunity for IT teams to protect data more selectively based on a classification model that meets unique business and security needs.

Many companies use a relatively simple model that classifies data into three categories—public, confidential and restricted—and also take into account the device and platform used while other businesses have a much more complex classification model and also take into account many more factors such as user role and location.

The data model deployed should take into account both data classification and device type. IT teams should also want to layer additional considerations such as device platform, location and user role into their security policy. By configuring network access through enterprise infrastructure for confidential and restricted data, IT teams can capture complete information on how people are using information to assess the effectiveness of your data sensitivity model and mobile control policy.

Clear about roles and ownership

Who in your business will own enterprise mobility? In most companies, mobility continues to be addressed through an ad hoc approach, often by a committee overseeing IT functions from infrastructure and networking to apps. Given the strategic role of mobility in the business, and the complex matrix of user and IT requirements to be addressed, it's crucial to clearly define the structure, roles and processes around mobility. People should understand who is responsible for mobility and how they will manage it holistically across different IT functions. Ownership needs to be equally clear when it comes to mobile devices themselves. Your BYOD policy should address the grey area between fully managed, corporate-owned devices and user-owned devices strictly for personal use – for example:

- Who is responsible for backups for a BYO device?
- Who provides support and maintenance for the device, and how is it paid for?
- How will discovery be handled if a subpoena seeks data or logs from a personally owned device?
- What are the privacy implications for personal content when someone uses the same device for work?
- Both users and IT should understand their roles and responsibilities to avoid misunderstandings.

Build compliance into the solution

Globally, businesses now face more than 300 security and privacy-related standards, regulations and laws, with more than 3,500 specific controls. Therefore it is not enough to simply try to meet these requirements, businesses need to be able to document compliance and allow full auditability.

Many businesses have already have solved the compliance challenge within their network. The last thing the IT department wants to do now is let enterprise mobility create a vast new problem to solve. Therefore IT departments should make sure mobile devices and platforms support seamless compliance with government mandates, industry standards and corporate security policies, from policy- and classification-based access control to secure data storage. Your EMM solution should provide complete logging and reporting to help you respond to audits quickly, efficiently—and successfully.

Prepare for the future

Don't write your policies for only today! Keep in mind what enterprise mobility will look like in the next few years. Mobility, devices and users' needs will continue to evolve and expand the potential of mobility, but they will also introduce new implications for security, compliance, manageability and user experience.

IT departments need to pay attention to ongoing industry discussions about emerging technologies like these, and design their mobility strategy around core principles that can apply to any type of mobile device and use case. This way, they can minimize the frequent policy changes and iterations that may confuse and frustrate people.