white paper - white paper - white paper - white paper - white paper - white paper - white paper

smartphone management

Business Services

orange™

enterprise challenges in smartphone management

Smartphones are revolutionizing the workplace but, without a rock-solid management infrastructure in place, they threaten to overwhelm the IT department and blow a hole in enterprise security. No longer able to simply provide a laptop for computing and a BlackBerry for email, the IT department needs to exercise control over settings, security, connectivity and software over all mobile devices in the organization.

It took over a decade, but smartphones are now accepted right across the enterprise. Managers routinely expect their employees to be able to collaborate, access corporate applications, or at least check email, when they are out of the office, all in the name of productivity improvement.

Their usage is not limited to knowledge workers, executives and IT experts, either. All employees want to benefit from the productivity improvements that mobile devices can deliver, and they are found in all job roles from truck drivers to oil rig workers.

This smartphone push isn't just driven from the top, because employees are also keen to use them. A Market Pulse survey from IDG Research found that 74% of employees wanted real-time access to critical business information through their mobile devices. They are even willing to use their own devices for this, with 59% of employees actually asking to do exactly that!

Basic applications including email, calendaring and contacts on smartphones or mobile access to CRM and ERP systems are actually just the beginning of the mobile application revolution. According to IDG Research, 39% of businesses are already considering deploying next-generation applications with consumer-like functionality.

These include using GPS, the camera and social networks to help employees in their day-to-day work. A marketing executive, for instance, may use a device to photograph a competitor's billboard and tag it in a database for market research, or he may use social networks to access information during a meeting.

new challenges

As smartphones become an indispensable business tool, they also become a management headache. Some of the management challenges include:

- IT departments in the finance sector will want to disable the camera on all employee devices in order to guarantee data confidentiality
- financial controllers will want monthly reports on their mobile assets, such as number of devices, type and usage
- government institutions will want to ensure that data on their employees' smartphones is encrypted to avoid any damaging data leaks

In the past, most IT departments tried to manage the increased complexity of mobile devices by limiting the number of platforms supported, such as a Black-Berry for smartphones and Windows laptops for mobile computing. However, this approach has become unsustainable, particularly with the flood of consumer-type devices into the workplace.

Even if enterprises did push ahead with this strategy, how would IT departments counter the flood of non-approved devices into the organization? There is also a risk that a restrictive mobile strategy would result in poor adoption of the service, damaging the return on investment (ROI) of the technology project.

And why should the IT department even stand in the way of employees who actually want to use their mobile devices to be productive? The early arguments that iPhones are not suitable for enterprises are no longer valid, with the platform now offering extensive device management capability. Some applications work better on some platforms than others, so a plurality of platforms can help ensure the right tool for the right job.

figure 1 – business challenges driving mobile device management

help the IT department cope

So what does this all mean for the beleaguered IT department? Clearly the mobile enterprise needs the same support as offered to standard PCs. As mobile devices have become more complex, they have the same issues as PCs, such as data security, data management and application support. And with companies embracing more than just one mobile platform, the IT department will have to invest in tools that can manage mobile devices powered by Android, BlackBerry, Windows Mobile, Apple's iOS and Symbian.

Typical mobile device issues that IT departments will need to manage include:

- assets and settings
- passwords and security
- connectivity control
- software deployment and updates

Although many of them are familiar with rolling out and supporting applications on laptops and PCs, mobile devices are not usually connected to the corporate LAN and do not use a standard PC image.

Perhaps the biggest potential management headache for IT departments is security. With smartphone memory averaging 8GB, employees have enough potential to put a massive volume of key corporate data at risk through a compromised device or by losing it altogether.

Designing a security policy is crucial for mobile application deployment as it gives enterprises the platform and confidence to do so much more with their mobile strategy. The security strategy needs to cover the three cornerstones of security:

- confidentiality: ensure that data is not shown to the wrong people
- integrity: ensure that it is not possible to make unauthorized changes to either data or the system
- availability: ensure that the data is available at all times for authorized users

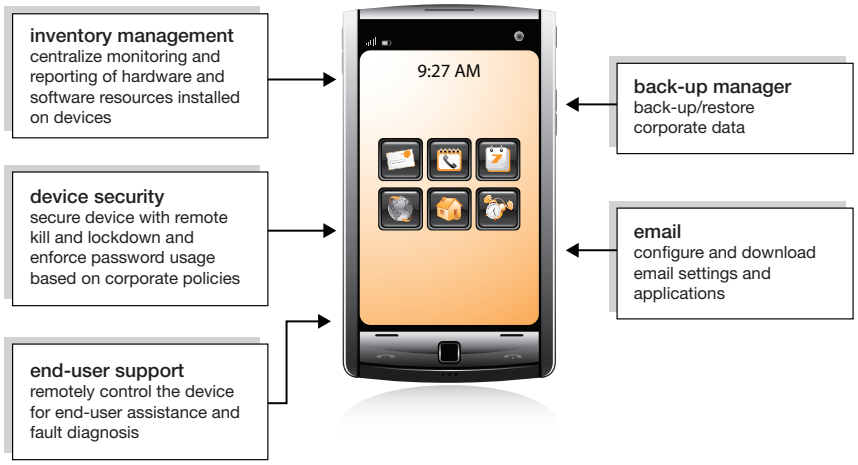
Security tools need to be able to support a range of activity such as patch management, keeping applications secure with no vulnerabilities, protecting against malicious code and blocking unauthorized device access to corporate resources. In addition, they need to give the enterprise the ability to remotely lock or wipe devices and enforce the encryption of confidential company data.

over-the-air

Physically accessing all mobile devices in order to deploy applications or change settings is nearly impossible in a global organization. It may not even be practical when the device is first brought into the organization, because the mobile device itself may well be the user's own. And relying on employees to deploy applications via the PC and USB cable is not the best approach for either users, who may not be particularly IT literate, or the IT department, who would not have enough control over the activity.

The alternative is to use specialist mobile device management (MDM) and security tools that can automate device configuration, support, administration and security all over the air. This means that all device management activity, from deploying applications to turning on or off functionality, such as the camera, can all be carried out by sending a simple system SMS message with no user intervention required.

figure 2 – what to look for in a mobile device management solution



MDM tools also provide asset management, which is a key activity for mobile devices, particularly with refresh cycles being as frequent as every year. This gives the IT department knowledge of what mobile devices are being used and what applications and versions are loaded on them and allows it to cope with the lack of a standard image or smartphone configuration.

Ultimately, MDM gives enterprises the tools to maximize the benefits of their mobile strategy. By providing a framework to manage all types of mobile devices over the air, IT departments can deploy applications across the entire estate, irrespective of the mobile network or device operating system and with no user intervention required. It allows them to ensure security by patching application vulnerabilities, keep data safe with encryption and apply the security policy across smartphones, whether supplied by the company or the user. And finally, it provides them with a detailed up-to-date view of all mobile devices and applications within the organization.

for more information, visit
www.mnc.orange-business.com

regional offices

Americas

Atlanta
600 Galleria Parkway
Atlanta, GS 30339
USA
Tel.: +1 866 849 4185

Washington, D.C.
13775 McLearen Road
Herndon, VA 20171
USA
Tel.: +1 866 849 4185

Europe

Paris
7 chemin du Cornillon
93200 Saint Denis
France
Tel.: +33 1 55 54 20 00

Slough
Betjeman Place
217 Bath Road
Slough, SL1 4AA
United Kingdom
Tel.: +44 (0)20 8321 4000

Asia Pacific

Singapore
Block 750 Oasis
Chai Chee Road #04-02
Technopark @ Chai Chee
Singapore 469000
Tel.: +65 6 517 1000

Business Services

orange™