The Challenge
Mobile working has found favor with employees at companies around the world, and many employers are realizing the advantages of this growing trend. According to CBI, the UK’s business lobbying organization, there is evidence that the number of people working from home is on the rise. A total of 59 percent of employers who responded to a survey in 2011 offered teleworking, up from 13 percent in 2006*. Modern technology solutions such as cloud storage allow employees to access corporate information from anywhere at any time, which helps employees achieve a work-life balance. Many companies want to provide employees with this kind of flexibility; however, they are faced with the challenge of safeguarding sensitive information on mobile devices.

The Client
reed.co.uk is a leading recruitment website in the UK. The firm highlights vacancies from more than 10,000 recruiters and 4.5 million job seekers rely on reed.co.uk in their search for employment. More than 100,000 job applications are submitted to the website every day.

In 2012, the company replaced its enterprise legacy systems with a browser-first strategy, which allows information to be easily accessible through mobile devices. “We don’t believe in the concept of ‘behind the firewall,’” said Mark Ridley, director of technology, reed.co.uk. “Our systems should be available globally and in the cloud. Our next step will be a set of mobile-first solutions, but in the meantime we’re ensuring that our employees have the ability to use their mobile devices to access line-of-business applications including emails, Salesforce.com and our intranet, Jive. Addressing mobile security concerns is crucial us.”

The company currently manages a fleet of 20 corporate-owned and 60 employee-owned smartphones and tablets, which includes a range of operating systems. reed.co.uk’s key requirement for an Enterprise

Solution Overview
- Customer: reed.co.uk
- Industry: Recruitment
- Geography: UK
- Features: BYOD, MDM
- Devices: 1-100
Mobility Management (EMM) platform was to keep mobile devices secure, while supporting the user experience and ensuring that users can access the full features of their personal phones.

After evaluating a number of EMM providers, reed.co.uk chose AirWatch® due to its ease of use and streamlined user experience. “Our employees are very technical and will immediately notice intrusive solutions that require a lot of system resources,” said Ben Jackson, technical operations manager, reed.co.uk. “AirWatch does everything we need it to do, without being intrusive or restrictive.”

**The Solution**

reed.co.uk cloud strategy ensures that in terms of business continuity and disaster recovery, the company no longer has to rely on one office location. The company has adopted a role-based access policy to corporate data and applies device management policies based on device ownership. The company enables corporate access from personal devices on an opt-in basis and combines a wide range of Bring Your Own Device (BYOD) options, including Android, iOS and Windows Phone, with corporate-owned devices. “We only provide corporate-owned mobile devices to employees who need them for outbound calling,” explained Mr. Ridley. “Access to corporate data for all other employees is provided through our BYOD program.”

According to Mr. Jackson, implementing AirWatch was easy and employees are grateful for the ability to protect corporate and personal information, especially in the event that a device is lost or stolen. “Almost every day, employees at reed.co.uk ask me whether they can enroll their personal devices in AirWatch,” said Mr. Jackson.

An increase in user satisfaction, a reduction of costs related to corporate-owned devices and enabling employees to access corporate information from mobile devices adds to reed.co.uk’s modern and dynamic approach to technology in the workplace. “The security that AirWatch provides is the most important benefit for our company,” said Mr. Ridley. “AirWatch enables us to push information further into the cloud and provides us with a fundamentally secure architecture we can build on.”

*Navigating choppy waters: CBI/Harvey Nash employment trends survey, CBI. 2011*