Mobile Device Management: Choosing the Right Platform for Your Business

Unlike many large enterprises, San Francisco-based Union Bank was ahead of the curve when it came to managing mobile devices. As a full-service commercial bank with some 2,500 mobile users among more than 11,000 employees in 401 branches primarily in the southwest, Union Bank put mobile policies in place a few years back for its corporate-issued BlackBerry smartphones. But things changed when new smartphones came along and employees began demanding them. Steve Chong, manager of messaging and collaboration at Union Bank's facility in Monterey Park, Calif., found a way to embrace the new mobile devices, but had to come up with a new mobile management strategy to do so.
"From our IT standpoint, we are ahead of the bubble with all these phones coming in, because we can say to our users, 'Yes, we can support these phones,'" says Chong. "And of course our user population loves that—they can get their own phone models and we can support them," he adds.

The new strategy is to make all mobile devices "employee-liable," so that employees choose their devices and take greater responsibility for them. To implement this new approach, Chong selected Good Technology™’s Good for Enterprise™ mobile management software, using it alongside RIM’s BlackBerry Enterprise Server.

Union Bank is not alone. While a few years ago BlackBerry was the standard when it came to corporate-issued devices, the landscape has changed as iPhone and Android fever has spread. That has meant a shift from device uniformity to operating system and form-factor fragmentation. Not only that, but employees want to access corporate data on these new tools so they can work anytime, anywhere. So it’s no surprise that getting a handle on these disparate mobile devices and the data on them has become a real headache for IT departments. While corporate-owned smartphones, laptops and tablets can be locked down, IT staff now have to contend with smartphones and tablets from different vendors on a variety of platforms, and worry about coming up with policies to deal with a plethora of issues including security, liability, bandwidth considerations and software distribution, as well as providing users with a consistent corporate experience.

"Companies are looking to enable consumer devices other than BlackBerry," says Jonathan Fischer, director of the MDM Industry Solutions Practice team, at AT&T. "Android and iPhone are proliferating in the enterprise, and management is trying to figure out how to gain control of these consumer devices, along with the burgeoning number of tablets that are also being used at work," Fischer says.

Although these mobile devices are not replacing PCs on a full-time basis, their ever-increasing processor power and memory are enabling them to take on the role of primary communications device, according to market research firm Gartner. But many organizations, government entities and businesses around the globe are finding that their IT staffs do not have the skill sets to manage mobile platforms and applications. The issue doesn’t just apply to U.S.-based businesses; it affects enterprises in other countries whose employees bring

---

**Elements of MDM**

- **Software Distribution**—The ability to manage and support mobile applications. Tasks include deployment, installation, updating, deletion and blocking.
- **Policy Management**—Development, control and operation of enterprise mobile policy.
- **Inventory Management**—Including provisioning and support.
- **Security Management**—Enforcement of standard device security, authentication and encryption.
- **Service Management**—Rating of telecom services.

Source: Gartner Inc.
their consumer devices to work. As a result, organizations are turning in increasing numbers to outsourcing for mobile device and service management. Mobile Device Management (MDM) involves software or services that manage smartphones, laptops and tablets, and includes support for inventory, provisioning, configuration management and software distribution. MDM suites, according to Gartner, often include specific requirements such as security and bandwidth management, and are not always well-supported by tools and systems designed for PCs.

According to an April 2011 survey by VDC Research, end users in organizations both large (65% of >$1 billion in annual revenue respondents) and small (52% of <$1 billion in annual revenue respondents) said that they were “very interested” in outsourcing a broad range of enterprise-grade mobility tasks, including device monitoring, systems integration, mobile application services, security assessments and monitoring, and self-service portals.

The key drivers, VDC Research found, were device proliferation, lack of in-house skills, the need to simplify the end-user experience, and anticipated costs savings.

**Corporate mobile challenges**

When managing consumer devices in the enterprise, companies need to be mindful of device control, including the ability to locate, lock and wipe devices that may be lost or stolen, says Fischer. Configuring and deploying applications is also a challenge, he says. Beyond that is governance, which includes the question of how to separate individual responsibility from corporate responsibility.

“It is important to be able to separate corpo-

---

**A partner in mobility**

Every day, enterprises around the world are receiving requests to support more mobile devices because of the productivity improvements and total cost of ownership benefits they provide. At the same time, many are finding the corporate-liable, standardize-on-one-OS model does not work for them. Many organizations also lack the in-house skills to support mobile applications and platforms, and do not know how to:

- Simplify the end-user experience to ensure adoption
- Meet high expectations for cost savings

If mobilization of your business is imperative, choosing the right solution can be overwhelming as the number of vendors and platforms in the mobile device market continues to grow and complexity increases. Regardless of the device and operating system, AT&T’s mobile specialists can guide you through the process, starting with understanding your specific needs.

“If a customer has high security requirements maybe they’re not deploying the bring-your-own device model. For some customers, a container solution is best, while others will require a different approach,” AT&T’s Jonathan Fischer explains.

AT&T also offers enterprises a mobility governance workshop, which includes a structured approach to preparing companies for the evaluation and selection of their mobility infrastructure. This allows them to not only put together the technical side of their mobile strategy but the policy side as well. “Every effective mobility deployment comes with a policy first, so I can ensure my folks understand what’s expected of them,” Fischer emphasizes.
rate data from personal data on these devices, and AT&T is solving this issue with best-of-breed solutions. Sometimes it becomes a policy issue where [employees] have to sign a policy stating that if something happens to the device, the entire device will be wiped and any personal data connected to corporate resources will be deleted," Fisher notes.

"If I’m an IT manager and mobilization of my business is imperative, that presents me with the challenge of keeping up with the different end points in my business and the different user scenarios that I have to manage," says Gavin Russell, associate director of Mobile and Device Management Solutions, AT&T Business Solutions. A key task for IT managers, he says, is to manage mobile devices so that users have a consistent experience that encompasses both productivity and protection, regardless of the device and operating system. And, he adds, the need for MDM is only going to grow, as more business functions are mobilized.

According to Russell, there are five key questions IT managers need to ask when building an MDM strategy:

1. What are my devices today, and what are they going to be tomorrow?
2. What are the things I want to be able to manage from a mobility perspective across those devices?
3. What level of security does my organization need?
4. What applications are needed in my enterprise now and in the future?
5. Do I want to manage this MDM strategy in-house or outsource it?

When help is needed
New York Life, America’s largest mutual life insurer, turned to AT&T when it realized it needed to provide mobile capabilities for its employees.

"We recognized that mobile devices—things like smartphones and tablets—were being more widely adopted by people in their personal life and there was going to be an impact on their business life," says Sean Mulligan, a corporate vice president at the company. "People were looking for ways to see if they could get to their corporate email so they wouldn’t have to carry a laptop around."

However, one of the main issues was control and standardization, especially when it comes to security.

"The only way you could set a policy and enforce that policy was to have an MDM-type tool that allowed you to control those policies being put on those devices," Mulligan says. After consulting with AT&T’s mobile apps consultants, the firm chose MobileIron VSP as its mobile management platform. AT&T also supports McAfee Enterprise Mobility Management (EMM) and Good for Enterprise from Good Technology.

Since his institution implemented its mobile strategy with AT&T’s assistance about a year ago, Mulligan says he has witnessed its benefits, as employees can get to their email and other corporate mobile data more quickly and can interact more with the people, information and systems they need to reach. "They have more accessibility on their terms, using devices they’re comfortable with," he says.

"Our product management team is continually working to vet the best products in market," says Russell. The three products currently in the AT&T portfolio were looked at for their commercial viability, features and ability to scale and grow with AT&T’s demands. They were also put through rigorous testing, he says. McAfee EMM and MobileIron VSP are both platform-based MDM products, so they manage the device all the way down to the OS level, while Good is container-based, he says. "It’s a high-security, very confined mobile device management solution and includes the ability to manage everything within a container," including dividing corporate data from personal data, Russell explains.