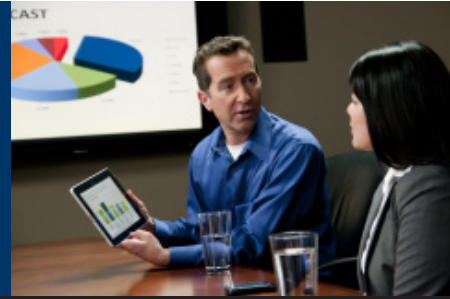


10 Reasons for Managed Mobility



PRODUCT DATASHEET

Mobile device management is creating unnecessary work and security headaches for IT departments across the globe. You don't have to suffer under the weight of this burden. Find out how Sybase Managed Mobility can take the worry and high cost out of making your enterprise mobile.

1 **MANAGE VARIOUS DEVICE TYPES COST-EFFECTIVELY.** It can be difficult to get all of your employees on board with a single OS. Yet, the cost to manage a diverse range of devices can be very high, especially when factoring the time it takes for IT to learn and support the differences between multiple operating systems.

Solution: A managed mobility solution such as Sybase Managed Mobility takes care of all that complexity for you, letting you support all mobile platforms easily and affordably.

2 **LIMIT RISK FROM STOLEN DEVICES.** A lost device is like a blank check: anyone can take it to the bank to withdraw your confidential data. Organizations need a safeguard against unauthorized use of lost or stolen devices.

Solution: By combining data fading and smart encryption technologies, Sybase Managed Mobility provides robust protection against unauthorized access to confidential data, even on devices that are out of reach.

3 **LIMIT RISK FROM UNTRUSTED APPLICATIONS.** End users will inevitably want to install third-party applications on their mobile devices, and these applications can be a target for viruses and malware. The risk is especially high when applications attempt to access corporate applications and data, which can lead to security breaches and device infection — putting more pressure on IT and raising support costs.

Solution: Sybase Managed Mobility enlists the use of black-listing and white-listing applications, as well as port control functionality to block external applications and prevent mobile devices from synchronizing with untrusted computers.

4 **CONFIGURE DEVICES OVER THE AIR.** Given time and resource constraints, IT departments cannot physically bring in every mobile device in order to configure them properly, and letting end users perform configuration tasks will likely result in issues that overwhelm support staff.

Solution: Sybase Managed Mobility lets administrators perform expert configurations without ever touching the physical devices. It also supports blocking of configuration displays and other settings from end users.

5 **RESTORE FORGOTTEN PASSWORDS EASILY.** If a user initiates a hard reset on his or her device, all data and specific settings on the smartphone — including passwords — will be lost, creating unnecessary work for your support and IT departments.

Solution: Sybase Managed Mobility includes multiple means of recovering passwords and even allows end users to generate their own temporary passwords.

6 FACILITATE CENTRALIZED BACKUPS FOR ALL MOBILE DATA.

Leaving data backups to end users is never a good policy, and mobile devices are no exception. Without backups to restore from, lost, stolen or malfunctioning devices can cause big headaches for users and IT.

Solution: Sybase Managed Mobility ensures proper safeguarding of user data through automated backups, provisioned over the air. The data is preserved in a secure, centralized location and can be restored quickly and easily.

7 STANDARDIZE MOBILE MANAGEMENT PROCEDURES.

The lifecycle of every mobile device has many phases, and each phase involves a laundry list of routine management and security tasks that hardly vary from device to device. How you bundle and assign responsibility for these procedures can make a big difference in labor efficiency.

Solution: Sybase Managed Mobility provides simple templates that help you assign tasks and batch jobs to different groups and individuals in order to maximize efficiency and ensure that all work performed adheres to corporate policy. The templates are so easy to use that you can be up-and-running in as little as 15 minutes.

8 LOWER DEVICE DATA TRAFFIC AND ASSOCIATED COSTS.

Mobile devices use large amounts of data which can lead to higher costs and affect device performance. These factors can lead to inefficient use and lower adoption of the devices.

Solution: Sybase Managed Mobility compresses the data sent for backup, minimizing data use. Sybase Managed Mobility also maximizes battery life from a central console.

9 PROVIDE ENCRYPTION.

Sensitive and high value data must be encrypted in case of loss or theft of a device. To be effective, the encryption must occur automatically and be as transparent as possible to the end user.

Solution: Sybase Managed Mobility provides individual file encryption or full device encryption using intelligent algorithms, allowing IT full control over how sensitive corporate data is protected.

10 REQUIRE CERTIFICATION FOR SYNCHRONIZATION.

Letting the wrong computer or third-party application synchronize device data can result in a major security breach, yet synchronization with Microsoft Exchange is sometimes appropriate.

Solution: Sybase Managed Mobility can help you ensure that only trusted servers and applications are allowed to synchronize with mobile devices by requiring a certificate before any communication with the Exchange server. Administrators can manually set the synchronization to require the certificates and the certificates can be distributed over the air to trusted applications.