U.S. Cellular® Presents

5 Reasons Your Business Needs **Mobile Device Management**

1. Data Security

MDM protects your data via remote device wipes on lost or stolen devices.

It automatically detects, prevents or blocks:

- Hacking and malware
- Unsecured networks
- Illicit data transfers
- Malicious Wi-Fi hotspots

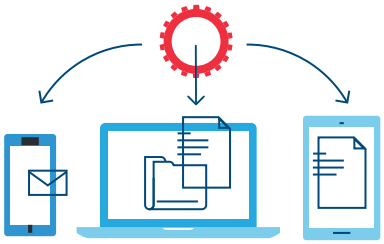
21% of companies have had a mobile security breach.[1]

2. App Synchronization

From a single admin console, you can remotely:

- Install or delete apps
- Update apps
- Push or pull data
- Edit user permissions

3. Cost Cutting



Bringing all your devices and software **under one umbrella** lowers your IT costs, because you don't have to invest in multiple solutions that work for just one type of device or operating system.

4. Employee Device Integration

64% of all employees use a personal mobile device for work.

MDM lets you enforce your organization's policies, even on employees' personal devices.

5. Device and Location Freedom

MDM empowers **a flexible and remote workforce** by allowing employees to use their device of choice. MDM enables **secure, standardized business practices**, regardless of device or location.

80% of companies rely on employee access to business applications on their personal devices.[2]

To find the best MDM solution for your business, partner with U.S. Cellular.
Visit **uscellular.com/business** or call **1-866-616-5587**.

Sources

1. Hamblen, Matt. One-fifth of IT pros say their company had mobile data breach. Computer World, 2016. https://www.computerworld.com/article/3048799/mobile-wireless/one-fifth-of-it-pros-say-their-companies-had-mobile-data-breach.html

2. Syntonic 2016 Employee Report: BYOD Usage in the Enterprise https://syntonic.com/byodresearch/

Business U.S. Cellular