WHITE PAPER

SECURE COMPANY INFORMATION ON EMPLOYEE DEVICES

A Guide to Choosing an MDM Solution

uscellular
BUSINESS

MDM streamlines your mobile workforce by remotely monitoring, managing and securing data across all your mobile devices, including company-owned and employee-owned devices.

MDM can:

- boost efficiency by remotely managing all devices—whether you have a few or a few thousand
- save valuable IT staff time by avoiding endless manual configurations
- share and synchronize content, applications and data across an organization's devices
- act as a security gateway to applications, devices and networks, with security features such as restricting apps and outbound communications, and the ability to remotely lock and wipe devices in the event of loss or theft

Business decision makers must consider their organization's needs carefully when choosing an MDM solution and provider.

What to Consider in a Mobile Device Management Solution

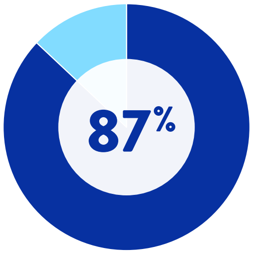
Given the basics of mobile device management, an MDM solution can be tailored and scaled to perform a variety of functions, from increasing the functionality of an Internet of Things (IoT) network to strengthening Bring Your Own Device (BYOD) policies in and out of the office.

Business decision makers looking to adopt MDM should consider the following factors:

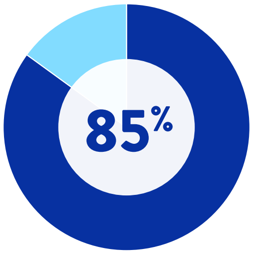
Business Size

The number of employees and type of workplace (remote, hybrid or in-office) affect a company's MDM procurement decision. Smaller businesses with fewer employees might be more concerned with maintaining an effective BYOD policy, while larger organizations might prioritize inventory management and data security.

At all levels, however, an MDM program can assist in managing and monitoring employee device usage. From small businesses to large corporations, many workers already use mobile devices for work purposes, with or without formal oversight.



87% of U.S. businesses depend on employees to access business apps from their private devices.[2]



85% of companies implemented BYOD policies because of COVID-19.[2]

Number of Devices

Like the number of employees, the number of mobile devices used within a company affects its MDM options. Businesses with a large number of devices in use should adopt a solution that supports inventory management, content synchronization and the ability to easily manage user permissions and access to applications.

The ability to remotely change permissions and wipe devices also helps manage higher volumes of hardware, including IoT equipment. An effective MDM solution can integrate IoT, desktop and mobile devices under a single umbrella.

Businesses with fewer devices, however, need to balance the probable use of personal devices against data security, employee privacy and effective device management. The number one concern employees have when it comes to BYOD policies is privacy. At least 74% of organizations have visibility into emails in devices under BYOD. This potentially infringes on employee privacy, which is why 38% of organizations do not want to adopt BYOD.[1]

At least

74%

of organizations have visibility into emails in devices under BYOD.[1]

68%

of healthcare data breaches were due to loss or theft of mobile devices.[3]

Device Types and Usage

MDM solutions are compatible with multiple operating systems (OS), including iOS, OSX, Android and Windows. This enables companies to integrate MDM across mobile devices, desktop devices and other equipment. Companies with desktop and mobile hardware, as well as those who use multiple operating systems, should adopt an advanced device management solution that includes support across platforms and types of devices. A company with a design team that uses OSX and an accounting team that uses Windows, for example, would benefit from an advanced device management plan that incorporates multiple operating systems.

Today's workforce is increasingly mobile and remote, and many employees use a personal device for business purposes at least some of the time. Often, the use of personal devices is necessary: 87% of U.S. businesses depend on employees to access business apps from their private devices. And 85% of companies implemented BYOD policies because of COVID-19.[2] Given these statistics, a sensible BYOD policy that prioritizes data security is the right move for a business with a remote workforce or one that uses mobile devices regularly.

Exposure and Liability Potential

Some businesses are more vulnerable than others to exposure, liability and profit loss from data breaches and lost or compromised devices. Businesses with heavy mobile device usage can be subject to increased risk. For example, a recent survey conducted by Bitglass found that 68% of healthcare data breaches were due to loss or theft of mobile devices.[3]

Where mobile data security is a top concern, MDM protects company data and employee privacy the most. Secure PIM containers keep corporate and personal data separate on devices within an MDM network. An effective MDM solution should also limit devices from connecting to unsecured networks.

Levels of Mobile Device Management

There is no such thing as a "one-size-fits-all" MDM solution. There are four categories or "tiers" of mobile device management, each with services that can benefit a variety of organizations. Each successive tier adds more functionality, and the upper levels include the features of those below. Most businesses can benefit from these basic capabilities, and many more can significantly increase productivity and efficiency by adopting an advanced solution.

1 BASIC POLICY MANAGEMENT

- Full device wipes
- Password protections

2 BASIC DEVICE MANAGEMENT

- Full and partial device wipes
- Public and private applications
- Inventory management for hardware and applications
- Basic support for iOS and Android systems
- Volume purchase programs for mobile applications

3 ADVANCED DEVICE MANAGEMENT

- Comprehensive iOS and Android management
- Desktop OSX and Windows support
- Role-based user administration
- User self-service portal
- Analytics support

4 ENTERPRISE MOBILITY MANAGEMENT

- Mobile application wrapping: adding policies to an existing app (like user authentication and usage restrictions)
- Software Development Kit to create custom applications
- Personal Information Manager to separate corporate and private data
- Secure web browser
- Mobile content push, pull and synchronization
- Location- and network-based restrictions
- Single sign-on

The 7 Elements of a Successful MDM Solution

To be truly effective, a mobile device management program should provide options for the following.

1. **EASY SECURITY POLICY MANAGEMENT**
   Security worries are among the biggest concerns for IT professionals considering MDM. To encourage buy-in from IT employees, security should be front and center.

2. **DEPTH OF AVAILABLE POLICY CRITERIA**
   Every organization has unique needs. An effective MDM solution has enough options and policies to allow a comprehensive solution.

3. **ENFORCEMENT OPTIONS.**
   Many employees can be hesitant to adopt MDM. To guarantee adoption and adherence to MDM policies, business owners should have access to a variety of enforcement options and choose the one that best fits their company.

4. **MONITORING CAPABILITY**
   MDM administrators should be able to continually monitor devices, even personal devices under a BYOD program, for noncompliance—without sacrificing privacy or security.

5. **SCALABILITY**
   An MDM solution should be able to evolve and grow with a business. Business owners should choose a solution that can easily and cost-effectively incorporate more devices and new device types.

6. **OPTIONS FOR BYOD**
   67% of employers support BYOD or plan to soon.[4] Any MDM solution should allow for the adoption and enforcement of a BYOD policy, even if one is not yet in place.

7. **EASE OF UPDATES**
   Poor usability can inhibit MDM adoption for employees. Onboarding, troubleshooting and system updates should be seamless and painless.

Choosing an MDM Provider

All of the above elements should be present in an MDM solution. Additionally, business decision makers should look for the following when choosing an MDM provider.

ONGOING SALES AND ENGINEERING SUPPORT

IT personnel and support fees are among the highest costs faced by businesses. And difficulty of use can be one of the biggest factors inhibiting employee buy-in. Therefore, an MDM provider should include technical support that continues well after installment.

STRATEGIC DIRECTION OF SOLUTION

Before choosing a provider, business owners must determine the specific issues to target with MDM. And the chosen provider should be able to work with the business to select a strategic, focused solution.

ABILITY TO CUSTOMIZE SOLUTIONS

Again, there is no one-size-fits-all MDM solution. The right choice for a business is the one that includes all the functionality that is required —and nothing extraneous.

In an increasingly mobile business landscape, mobile device management (MDM) allows business owners to streamline and control their company's device usage. The primary considerations when choosing an MDM solution are an organization's size, number of devices, the type and usage of those devices and the company's exposure and liability potential. A successful MDM solution includes options for BYOD, scalable growth, enforcement options and a streamlined update process. When choosing a provider, business decision makers should consider their strategic direction and their ability to find a custom solution, bolstered by ongoing support from the provider.

References

[1] FinancesOnline: 44 Basic BYOD Statistics: 2022 Market Share Analysis & Data
44 Basic BYOD Statistics: 2022 Market Share Analysis & Data - Financesonline.com

[2] ibid

[3] Lost and Stolen Mobile Devices Are Leading Cause of Healthcare Data Breaches
Lost and Stolen Mobile Devices Are Leading Cause of Healthcare Data Breaches - Kiteworks

[4] Techjury, 43+ Stunning BYOD Stats and Facts to Know in 2022
43+ Stunning BYOD Stats and Facts to Know in 2022 (techjury.net)

UScellular® offers a broad suite of MDM solutions to meet your unique business needs – all backed on a network with national coverage that works anywhere.

To learn more, call **866-616-5587** or visit **UScellular.com/business**

uscellular
BUSINESS