Enterprise-Grade Mobile Device Management: How to Ensure Your Data is Protected

Mobile devices provide unprecedented convenience and quick access to your employees. They also provide an equally unprecedented attack surface whether they work with issued devices or your organization's bring your own device policy.

As the COVID-19 pandemic caused millions of employees to become remote, poor security on home networks became a major risk. Now that society is reopening and remote work is here to stay, your organization is at risk once more as mobile devices freely roam public areas with insecure connections and opportunistic hackers.

To better manage the security of confidential assets stored on employees' mobile devices, organizations have turned to professional services to manage an MDM. Here's what you need to know about what your organization should and should not do concerning an MDM to ensure that data is kept safe.

What is an MDM?

An MDM, or mobile device management solution or service, is the process of securing the data on mobile devices spread across a workforce. While mobile devices like smartphones, tablets, laptops, and specialized devices make it easier for employees to perform their jobs and quickly communicate with teams and management, they also become literal walking security threats.

If an employee's device is lost, stolen, or hacked, malicious parties may get ahold of valuable business data. It can expedite the theft of trade secrets and proprietary intellectual property, or a large-scale breach of employee or customer data that can cause incalculable losses in either direction. IT executives must make an MDM a key component of managing technology risk in their corporate environment.

MDMs, be they automated and self-service solutions or managed services, put more control into IT departments' and administrators' hands to manage the security policies and settings of mobile devices carrying sensitive data. Rather than facing the risks of weak home networks and public Wi-Fi every time an employee has their devices on hand in these places, an MDM solution empowers administrators to place enterprise-grade security on each device regardless of whether it was issued or is a personal device.

What Type of an MDM Solution Should I Use?

An MDM focuses on issued and bring your own device phones, laptops, vehicle-mount devices, wearables, and other technology that could easily put sensitive information into the wrong hands. An enterprise mobility management solution (EMM) on the other hand is a broader form of an MDM that goes beyond the device, user, and data by deploying a scalable application that tracks endpoints and provides real-time insights on activities taking place with each device.

Unified endpoint management (UEM) is the integration of an MDM and an EMM by expanding the focus area to desktop machine security and the increase attacked surface presented by IoT like printers, "smart" coffee makers, and other devices on the network that are not necessarily mobile.

An MDM solution like SOTI Mobicontrol provides numerous other functions separate of security, like improve network speed and the ability to quickly deploy business apps for remote employees so that they can get their jobs done. SOTI Mobicontrol also has features like lockdown mode to prevent malware plus geo-fencing, so that employees can access specific features on their phones when they are in the designated area then lose access when they leave.

Organizations that deploy an MDM also tend to work with professional services to manage an MDM so that they can outsource this particular function in order to focus on more pressing IT matters.

What Should My Organization Do Regarding an MDM, and What Should We Not Do?

* **Do inventory all mobile devices.** Create a mobile device inventory and make sure it is updated quarterly, so that your team can efficiently audit all the mobile devices used in your organization. This will ensure you find the right MDM plan that can cover this number of devices.
* **Do include thorough information in your mobile device inventory.**In addition to device names, the designated owner or department should be recorded along with model and serial numbers, when the device was purchased, warranties, and if the device has undergone any maintenance or repairs.
* **Do track device usage.**Tracking mobile devices provides a more thorough understanding of how they were being used, and a very clear digital footprint that can be followed in the event of a cyber attack. Automated asset tracking systems can log fine details about how mobile devices in the inventory are being used in order to root out suspicious behaviors and find technical problems.

* **Don't neglect employees who brought their own device.** In order for these devices to be included in the MDM plan, the organization needs to enact policies regarding both usage and physical security and how these devices can be used for business off the premises.
* **Don't forget about integrating the MDM with other security systems**. MDMs use access control terminals for user authentication when they sign in or out of a device. If electronic access control is already being used, integrating an MDM with it means that the IT department only needs to manage one user database. Additionally, it provides a clearer picture of how people and devices navigate the premises so that deviant patterns can be watched in the event of a breach.
* **Don't stop tracking once employees hand in issued devices.** Content surveillance is how devices can still be monitored once they've been turned in. It's possible that a component could be missing when the device was turned in, and they can still present a security risk. By implementing content surveillance with your MDM, it can provide an extra layer of security in what's otherwise a hands-off automated process.
* ***Don't overlook password policies and authentication****.*As many newsworthy breaches and hacks have proved recently, a weak password that can be easily guessed is all it takes for valuable and sensitive information to be leaked to the public on a large scale. To prevent cyber criminals from accessing stored data, mobile devices need proper authentication. PINs and passwords should be appropriately complex for devices and accounts, and it must be written policy instead of a mere suggestion. Multi-factor authentication (MFA) can provide additional levels of protection that a strong password alone cannot, especially when ensuring that only the intended users are able to access the data.

PiiComm's MDM services fully support SOTI Mobicontrol and we can fast-track your organization to enterprise-grade security on all of your employees' mobile devices. Contact PiiComm today to request [a free mobility assessment](https://www.piicomm.ca/mobility-assessment/#mobility-assessment).