SWITCHING **MDM SOLUTIONS**

Migration Guide for Enterprises

Faronics

Executive summary

The use of mobile devices in the workplace has become common over the years. The productivity and cost saving advantages associated with mobile device use in a business setting are clear. However, this trend has resulted in various security concerns regarding the use of work phones. Enterprise data security breaches have grown massively in recent years. Most of these incidents were caused by the loss or security breach of mobile devices. While user-choice programs are becoming common in the enterprise, mobile devices still remain a primary attack vector to corporate security.

As a result, IT managers are always looking to find ways to securely manage these devices. The goal is to facilitate the use of personal devices while also keeping work and personal data both separate and secure. Dynamic organizations require a robust mobile device management (MDM) framework, but setting up an effective one can present multiple challenges to IT administrators.

69%

Cisco reported 69% of IT decision-makers favor BYOD as a positive addition to any workplace policy as it saves workers time.

87%

Research by Syntonic found that 87% of companies rely on their employees using personal devices to access business apps.

The changing needs of a business often require a revamp of certain technological solutions, and many organizations find that their current mobile device management framework isn't as robust as they would hope. This demands a change to a new system, but knowing exactly how to do so can be challenging.

Although there is no perfect roadmap that every single company can follow, there are specific steps that every organization must consider before changing mobile device management providers. The following is a combination of these considerations as well as some general information about switching solutions.

Identifying the MDM needs of an enterprise

At the end of the day, the entire point of switching from your current mobile device management solution is to better handle the needs of your enterprise. Therefore, the first step in your journey will be to fully understand what your organization needs from such a platform. According to technology marketing firm TechTarget, lost corporate mobile device represent a significant threat. Providing the ability to locate, lock, and potentially wipe lost devices must be available. For IT teams the scope tends to get gets slightly blurry when you move from corporate-owned devices to personal devices.

DETERMINE CURRENT MDM NEEDS AS WELL AS POTENTIAL FUTURE REQUIREMENTS

What goals does the company have for MDM implementation over the next few years?

Is an increase in the number of company-owned or personal devices expected in the future?

Will any aspects of employee productivity be affected based on upcoming goals?

While an MDM migration may seem complex, with Faronics, you're never alone during the transition. The following sections hopefully provide you with the insight and confidence necessary to break away from your previous solution and transition to one with the capabilities your enterprise environment needs.

Let's take a look at how enterprises should go about planning a switch to another solution.

Catering to user device preferences

The decision on which mobile devices are best suited for your business will depend on several key factors unique to your environment and user preferences. Device choice is also dependant on exactly how you plan on acquiring and distributing said devices into the hands of your employees. Although there are many ways to handle the distribution of mobile devices, there are some approaches that are fairly common like Bring-your-own-device (BYOD) and Choose-your-own-device (CYOD). BYOD is based on the fact that a vast majority of workers already own mobile devices suited for work. In fact, Pew Research recently found that

77%

of Americans own a smartphone

51%

of Americans own a mobile tablet

With so many employees owning their own mobile devices, it makes sense for a lot of companies to simply allow them to bring them into the office. Not only do these workers already have a familiarity with their own devices, but BYOD also brings these technology assets into the office without the company having to purchase the devices themselves.

BYOD or CYOD ?

There are downsides to BYOD. It can be hard for organizations to implement a mobile device management solution that keeps company data secure while allowing employees to use their own devices as they wish. The solution for many in this area is CYOD, which combines familiarity and security. Under this model, employees are allowed to pick the device they want to work with and the company will pay for it. While this gives the business more control over what workers can use the device for, it comes with a large upfront cost.

Both of these choices clearly have their positives and negatives, so the right decision will vary from company to company which might opt for a hybrid approach. Regardless, whichever is chosen, it will definitely impact how the IT team manages these devices.

Planning the switch

After reevaluating your existing MDM platform and have identified areas that need improving as well as elements of the current system you wish to carry over or drop completely, switching to a new MDM platform becomes more clear. IT managers need to take the following points into consideration, and create a migration checklist, while planning the switch.

01

PLAN YOUR MIGRATION SCHEDULE

The schedule should include critical milestones like fiscal dates, client contracts, product campaign launches, financial considerations, and factors impacting implementation success such as available budget.

02

PREPARE EMPLOYEES/ STAFF FOR THE TRANSITION

To ensure device users do not lose valuable time or critical work data, transparency into the MDM switching process is necessary. Inform them of the change and associated process beforehand.

03

CHOOSE THE RIGHT TIME FOR THE SWITCH

Choose a time when devices can be out of use to give IT teams time for the transition without impacting users. For example, the start/ end of a fiscal year emsures more devices available for implementation.

04

SET ASIDE TIME FOR TESTING AND TROUBLESHOOTING

It is important to allot time for testing throughout the migration process. This will help prevent any immediate issues from escalating further.

Migration checklist

- [ ] Create a manageable timeline for the entire process
- [ ] Evaluate and document existing workflows
- [ ] Prepare users for the platform transition
- [ ] Export assets from the previous MDM solution
- [ ] Notify all staff to conduct device turn in
- [ ] Un-enroll existing devices or perform device wipes
- [ ] Reassign previous Apple Device Enrollment Plan (DEP) and Volume Purchase Program (VPP) tokens.
- [ ] Re-enroll devices into the MDM platform using your preferred methods
- [ ] Conduct device assignments
- [ ] Check device inventory to ensure data transfer and device enrollment was successful

Ensuring seamless data migration

Although a robust mobile device management provider will make the transition as painless as possible, switching from a different vendor comes with the risk of lost data. Therefore, while you're making this change, you'll need to consider third-party file storage options. However, you shouldn't view this as a cumbersome chore. Rather, this can be a great chance for your IT team to improve data storage security. Specifically, this is a perfect opportunity to implement a 3-2-1 backup mechanism.

This backup concept speaks to the number of copies you have of each important piece of data. Under this umbrella, you should have three copies of all data using two different mediums (such as the cloud and a physical USB storage) as well as one copy that is off site.

The reasoning behind such a structured backup system is that data is the one resource an organization can't replace. If something were to go wrong during the transition, a massive data loss event could be catastrophic for the company’s well-being. Therefore, it's up to administrators to protect against these tragedies by being prepared.

Transitioning to Deep Freeze MDM

Change can be unsettling, especially when you've built up a routine to do your job effectively. However, with a transition as important as this one, it's important for employees to understand what's happening as well as why this change is occurring. The best way to combat any panic is by setting up a meeting with everyone who stands to be affected by this MDM switch. Exactly what point in the transitional process you decide to do this is up to you, but it might make sense to do it directly after you assess your company's needs.

With the right partner, the transition is usually seamless. Faronics has years of experience helping clients transition to their cloud-based platform. Deep Freeze MDM has an easy-to-use, intuitive console that can help IT admins enroll and deploy devices quickly and effectively. Powerful features help enterprise IT teams gain control and visibility over their mobile assets, allowing IT administrators to monitor and manage mobile devices from a single console. This takes a lot of the work out of deployment and maintenance, which helps minimize downtime and enhances employee productivity. Transitioning from one vendor to another is certainly a challenge, but meeting this challenge head on is the best way to improve your current system.

Contact Faronics today to find out how a change to our platform can benefit your business.