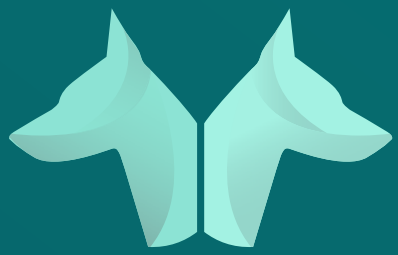

wireless watchdogs

A Guide to Implementing Mobile Device Management

Why. When. How.

wirelesswatchdogs.com | info@wirelesswatchdogs.com | (310) 622.0688

Introduction

The integration and usage of mobile devices in enterprise is expected to expand at exponential rates in coming years, with the Enterprise Mobility Market expected to be worth $73.3 billion by 2021. Over half of all enterprises were expected to embrace mobile device usage by 2017, according to Gartner, and in 2016 enterprises within the U.S. spent as much as $1,804 per employee mobile device annually.

The rapid arrival of mobile and connected device initiatives over the past few years has triggered the use of thousands of unmanaged and unsecured devices with access to critical data and information across the enterprise -- and now with the growth of the Internet of Things, even more unmanaged devices are starting to appear across enterprises, taking business risks to an even higher level.

EMM (Enterprise Mobility Management) and MDM (Mobile Device Management) solutions have surfaced in response to the rapid rise of mobile and IoT initiatives in enterprise. A 2017 Radicati Group report forecasts that worldwide revenues for the EMM market will reach more than $3.3 billion annually by the year 2021, achieved via an average annual growth rate of 18% over the next four years.

The growth in the popularity of EMM and MDM solutions is driven by the number of benefits that business can realize through the adoption of such solutions.

EMM & MDM Enterprise Solution Benefits:

- ☑ The ability to track all devices accessing corporate data and information
- ☑ Secure wireless access on individual devices and other network security features
- ☑ Security systems on devices that separate company apps from personal apps
- ☑ Capability to remotely lock a device that's been lost, wipe any sensitive data from a stolen device, or restore functionality to a found phone with backed-up data
- ☑ Logging and reporting capabilities for end-user activity
- ☑ Cloud-based platform options that are lower cost and easier to configure and manage

However, even with all the benefits current EMM and MDM solutions offer enterprises, MDM can be quite complex -- and definitely requires a business to do its due diligence when considering solutions. Enterprises still need to establish their MDM goals and requirements, for example, choose and implement the right MDM solutions for their specific organizations, and keep all devices and data secure.

This whitepaper will highlight these and other challenges with implementing an EMM or MDM solution, and how enterprises can overcome them.

Establishing MDM Goals and Requirements for an Organization

Establishing requirements and goals for MDM across an enterprise-sized organization can be problematic. Technology is constantly evolving, data types are constantly growing and changing, industry trends come and go, departments expand and divide, and security threats are constantly morphing with the newly-acquired skills of hackers. Also, data and security compliance guidelines across industries and global regions are also continually being updated as technology, data types, and security threats change.

With all of the complexities of the enterprise environment, creating an MDM strategy that clearly establishes goals and requirements for an organization is critical to overcoming the difficult task of getting everyone on board and on the same page.

An MDM strategy should include:

- ☑ A user-centric, cloud-based platform
- ☑ Security and regulatory compliance requirements an organization already has in place, as well as those it needs to incorporate in the future
- ☑ Network and service management considerations
- ☑ Endpoint management for all mobile devices, including IoT devices
- ☑ Specifications for mobile operating systems and devices that are already in use
- ☑ List of reporting capabilities that the organization needs
- ☑ Security solutions that are entirely comprehensive
- ☑ The ability to grow and change with the ever-changing needs of an organization
- ☑ Desired outcomes of implementing the MDM solution -- e.g., increase of mobile device security across the board, greater user accessibility, lessening IT help center expenses, etc.

Once an organization establishes overall requirements for mobile devices, the regulations that need to be followed, and what they want to accomplish, it'll be easier to build a strategy that's designed around those requirements and goals.

Choosing and Implementing the Right Managed Mobility Services

A multitude of Managed Mobility Services (MMS) have appeared in the past two years alone to help enterprises with their MDM strategies. MMS solutions were created to help an enterprise manage everything from their mobile apps to their mobile security networks. However, there are so many differing MMS solutions currently on the market that it can be difficult for enterprises to select the right one for them and their individual needs.

Choosing the wrong MMS solution can cost a business a lot of time and money if it becomes

clear at some point down the road that the solution doesn't actually serve the needs of the business. But according to recent Blue Hill research, choosing the right suite of Mobility Management Services can deliver a three-year return on investment of 184% -- and here are some things enterprise executives can do as they consider MMS solutions and determine which is the right one for them.

Determine Current Mobile Requirements

When considering different MMS solutions, the first thing an enterprise should do is determine if the solution will easily fit into their current landscape of applications and IT systems already being used. It should also be determined if the MMS fits the size and scope of the company's current needs and long-term objectives. Further, the MMS should be compatible with existing data and mobile device security networks and requirements, too, as well as the operating systems most users will have on the mobile devices they'll be using. Additionally, an MMS solution should be both flexible and scalable, and be able to grow with the changing needs of an enterprise.

Ensure the MMS has the Appropriate Integrations and is Customizable

The right MMS will have all the integration capabilities the business needs, with little to no need for manual processes. The MMS should integrate efficiently with all other existing IT management systems within a company, such as directory services, reporting systems, content management platforms, email and mobile app managers, security applications—as well as their cloud services, their mobile device security systems, and their entire mobility strategy.

An MMS should also be able to be built entirely around an enterprise's current IT infrastructure and support as little or as much as the company needs once it's deployed. MMS solutions that allow a company to customize their services and pay for what they need and not what they don't should always be at the top of the list.

Choosing the right suite of Mobility Management Services can deliver a three-year return on investment of

184%

Look for MMS Providers with Good Track Records and Reviews

It is imperative for enterprises to consider MMS providers that have stability and a good customer service track record. Some MMS providers will come and go quickly as the overall MMS market continues to fluctuate, which can leave customers stuck working with one provider one day and an entirely different one the next. Deciding on an MMS provider that has remained with most of their customers for a longer amount time will be ideal for companies that need a loyal provider.

Companies should also check out reviews of MMS providers on social media and reliable business ratings sites. Having a consistent stream of positive customer reviews can mean an MMS provider will be reliable and customer-service oriented.

Find Out What Kind of Support the MMS Offers

Last, but certainly not least, companies should find out what kind of support an MMS offers and whether their organization will have the bandwidth to handle the load. Determining whether the MMS provider offers 24/7/365 international support to their customers is also important, especially for enterprises with an extended remote workforce that has operations in locations across the globe -- and is a strong indicator that the provider will be able to save a business money by reducing help center and support costs, instead of generating new costs and expenses.

Security

Security is -- quite properly -- a huge concern for MDM for business. 94% of companies expect the frequency of mobile attacks to increase in the near future, according to a 2017 survey of security professionals conducted by Dimensional Research. 64% of companies were doubtful they would be able to prevent a mobile cyber-attack, and over one third of companies are failing to adequately provide mobile device security within their networks and across devices.

Gartner is predicting that investments in security products and services will reach $93 billion, which is a 12% increase over this year's record-breaking investment.

94%

of companies expect the frequency of mobile attacks to increase and 64% were doubtful they would be able to prevent such an attack.

Businesses are investing more money than ever before, specifically in mobile device security and mobile network security, as more employees start using personal devices and multiple devices at once to access valuable company information. They're also investing more money in mobile device security as cyber attackers continue to get more sophisticated in their abilities to create malware and spyware that has the potential to leak confidential data and destroy a company's entire brand and reputation.

However, a lot of companies are leaving their data and devices at risk because they don't have a solid mobile security strategy, and because they're not sure where the weakest links are in their mobile security network. To bridge their mobile security gaps, enterprises should generate a comprehensive mobile security strategy, and should always be aware of where they are most vulnerable.

A Comprehensive Mobile Security Strategy Should Include These Key Features:

- ☑ Initiatives to combat all current mobile threats, as well as emerging threats
- ☑ Well-managed cloud networks and applications, as well as wireless networks
- ☑ Two-factor identity authentication across mobile devices
- ☑ Intense focus on securing data itself with encryption and by restricting apps that can access it
- ☑ Compatibility with all MDM systems and solutions being used to manage devices
- ☑ Agility and flexibility to adapt to end users, technology, and emerging risks

Ready to learn more about the benefits of a managed mobile solution?

Please contact us for more information about how Wireless Watchdogs can help make your future less costly and more secure.

(310) 622.0688

info@wirelesswatchdogs.com

Conclusion

Consistent with Blue Hill Research estimates, unmanaged direct mobility costs can be 20% greater when compared to a managed mobile environment. For the average billion-dollar revenue company, telecom and mobility costs average $5-10 million per year, making effective MDM a million-dollar savings opportunity.

A lack of an MDM strategy that clearly establishes goals and requirements, choosing and implementing the wrong MMS solution, and a lack of a comprehensive mobile security strategy are the biggest threats to an enterprise's MDM. Fortunately, enterprises will be able to circumvent those threats and save millions of dollars after implementing the appropriate strategies and solutions mentioned in this whitepaper.

About Wireless Watchdogs

Since 2001, Wireless Watchdogs has been providing customized solutions that turn businesses with mobile device challenges into loyal customers. We work with companies in a range of sizes and industries, because we know optimized mobile systems are critical whether you are building houses, taking care of patients, or trading stocks.