International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 10 Issue: 10 | Oct 2023 www.irjet.net p-ISSN: 2395-0072

Mobile Device Management and Their Security Concerns

Khaja Taiyab Mohiuddin

MS Cybersecurity & Networks, University of New Haven, CT, USA (analyst133@gmail.com)
MBA Human Resource & Information Systems, Osmania University, Hyderabad, TS, India

---

Abstract - *Recently, enterprises and organizations have gained attention in mobile device management. This paper broadly discusses mobile device management by looking at various research papers and articles that have been published. This research paper will discuss theories and practices of mobile device management in terms of what it is and how it initiated its functions, and a comparison between MDM, UEM, and EMM. The paper discusses the bring-you-own-device policy compared to company-owned devices and mobile device management segmentation in cloud-based and on-premises operations. It discusses mobile device management features, elements, security concerns, and implementation. The mobile device management landscape overview, its importance, advantages, and the current industry market overview, are also discussed.*

Key Words: Mobile Device Management (MDM), Unified Endpoint Management (UEM), Enterprise Mobility Management (EMM), Bring Your Own Device (BYOD), On-premise solutions, Cloud-based solutions, Security concerns, Device management features, Device management elements, Corporate infrastructure, Employee productivity, Policy Compliance, Application Management, Remote monitoring and control, Network segregation, Compliance policies, Security protocols, Containerization, Deployment models, Automation, Data Security, Industry overview, Market segmentation, Efficiency and productivity, Regulations and compliance.

1. INTRODUCTION

Mobile device management is a broad concept in technology that involves the management of usage and implementation of mobile devices and associated policies in an organization. The main aim of adopting and incorporating mobile devices into the organization's computer infrastructure is to improve efficiency and increase employee productivity. Mobile device management enables companies' employees to use either company-owned or personal mobile devices to perform critical business operations while maintaining high-level security and policy compliance. Moreover, mobile device management can be implemented in different computing segments, such as on-premises and cloud-based solutions. It offers several advantages to the company. Additionally, there are several elements of mobile device management and the standard features of an effective solution. It has been an evolutionary technology, improving complexity and manageability over time.

The following sections expound on theories, technical intricacies, and practical considerations pertaining to mobile device management, shedding light on its indispensable role in contemporary corporate landscapes.

2. Theory and Technical Data

Mobile device management is the process of mobile device administration in terms of security and usage through third-party products that offer mobile device management features (Ortbach et al., 2014). Mobile devices, including smartphones, tablets, laptops, and other personal digital assistants, can be managed. It enhances end-user device management by deploying applications, policies, certificates, and infrastructure. The main aim of mobile device management is to provide solutions that enhance functionality, supportability, and security in a corporate environment while increasing employee performance and productivity.

The eruption of affordable and sophisticated mobile devices has drastically changed the computing environment. Some corporate information technology environments have entirely replaced desktop computing with mobile device computing. With the advancement of technology through the introduction and successful implementation of cloud computing solutions, some companies have fully embraced mobile device computing and done away with desktop computers. Cloud computing allows employees to access resources such as applications, data, and company databases entirely through mobile devices anywhere they have an internet connection. Adoption of computing models like this requires crucial implementation of mobile device management.

Users have slowly but steadily evolved into the preference of using computing devices and supporting software such as operating systems. Corporate information technology infrastructure in many companies has had to evolve to accommodate these changes. In the process, a new and unique set of challenges in information technology have arisen in companies due to the need to connect these mobile devices with internal computer infrastructure. Mobile device management has called for more attention because of the increasing and rapidly evolving complexity. Organizations must implement robust mobile device management frameworks to address associated challenges, including risk mitigation, costs, operational efficiency, and security breaches (Afreen, 2014). Segmentation can administer mobile device management components for specific user groups within the organization.

The implementation of mobile device management solutions may either be cloud-based or on-premises. Cloud-based mobile device management solutions are offered as software-as-a-service (SaaS) models. Cloud-based are preferable because of their flexibility, ease of configuration, less time to set up, and lower running costs because of regular and more manageable updates. On the other hand, on-premises mobile device management solutions are offered with the organizational computing infrastructure. Usually, they require additional hardware, virtual machines, and regular software updates, which may be more costly, thus leading to higher operational costs.

2.1 Functions of Mobile Device Management

One of the main functions of implementing mobile device management in corporate entities is enforcing uniformity across the organization's various user devices. It ensures a consistent configuration across all devices and their associated applications, including their functionality as well as conformity and compliance to organizational policies. Additionally, mobile device management enables information technology managers in corporate entities to saleably update resources, devices, equipment, policies, procedures, functions, and applications (Hayes et al., 2020). This reduces the time to update individual devices with various features, such as the underlying utility and operating software. Moreover, mobile device management solutions ensure that applications in the organization consistently conform to policies and procedures. Another core function of mobile device management is to track and monitor onboarded devices to get vital information that enables the company to effectively run its business functions, such as device location, functionality status, activity logs, and ownership status.

Mobile device management offers a solution to collectively perform this function without the need to involve the intervention of the device owners or vendor permissions and access certificates and protocols for every individual device. In addition, the mobile device management solution functions as an enabler for checking, diagnosing, monitoring, and troubleshooting devices remotely and regularly. This is mainly important because of the involvement of diversified device types. Over-the-air distribution of computing components, including database access protocols, company network protocols, certificates, applications, and other utility functionalities, are made possible through mobile device management solutions. Configuration and management of these resources can be done on various mobile devices, including tablets, smartphones, PDAs, printers, and mobile point-of-sale devices that can be company-owned or employee-owned.

2.2 UEM, EMM, and MDM

Mobile device management has, in recent years, evolved to become more than just a mobile management platform due to the inclusion of laptops and desktop computers on the list of supported devices. It has made it a primary device management practice regardless of mobility. This forms a basis for three device management solution models, namely: mobile device management (MDM), enterprise mobility management (EMM), and unified endpoint management UEM). The mobile device management model predominantly covers tablets and smartphones whose underlying operating systems are mainly Android and iOS. It allows complete management of these devices, including applications and application management, device configurations and security control, and access protocols and certificates (Tairov, 2019). They can enable corporate entities to deploy company-owned devices such as mobile phones to employees and give them a framework to manage those devices effectively. However, management is not limited to devices, as it may involve deploying single point-of-use information technology resources such as applications, self-service utilities, and point-of-sale resources.

On the other hand, enterprise mobility management (EMM) expands the scope of the mobile device management model to include the bring-your-own-device (BYOD) policy (Tairov, 2019). Bring your device is a solution that allows employees to onboard their own mobile devices onto the corporate information technology infrastructure. Enterprise mobility management solution enables organizations to manage employee-owned devices by implementing security, policies, protocols, configurations, and encryption of resources that involve corporate functionalities such as specific applications, database access privileges, emails, and other data contents. Organizations are then able to manage and monitor these devices and ensure they adhere to the policies and procedures stated by the company, as well as impose the consequences of noncompliance. Unified endpoint management (UEM) incorporates both mobile device management (MDM) and enterprise mobility management (EMM) to increase the scope of device management by addressing the challenges associated with more devices involved (Tairov, 2019). This model includes desktops and other Internet-of-Things devices and provides a framework for cross-platform management of devices, including data, software, utilities, configurations, and hardware from a single point.

2.3 Bring Your Device versus Company-Owned Devices

Penetration of mobile computing devices, especially smartphones, introduced the consumer demand for a bring-your-own-device policy, enabling company employees to use their own devices within the infrastructure (Steiner, 2014). This trend conceived more challenges that drove further interest in mobile device management. Among the challenges include finding the balance between enforcing company policies and protocols on those devices while maintaining a considerable degree of freedom and privacy for the owners. The company is concerned with securing its data and monitoring access to ensure policy compliance. In contrast, the employees are concerned with the company's ability to monitor their locations and other private activity logs on their mobile

devices. Mobile device management, however, provides a solution to prevent personal activity monitoring through its security settings.

Company-owned devices are easier to manage since they are not associated with the concerns emanating from employees' concerns in the case of employee-owned devices. However, corporate entities can use other methods to maintain privacy in employee-owned devices while enforcing mobile device management functionalities for the targeted components within the device. Containerization is one of the mechanisms that mobile device management solutions can use to secure their corporate components in the device while allowing the device owner the freedom and privacy to perform personal activities on that device (Jaramillo et al., 2013). While onboarding of employee-owned devices offers flexibility for users to utilize one device to perform work and personal activities, company-owned devices are considerably more secure and manageable in the company's interest.

There are solutions and policies used by large companies that allow employees to use mobile devices for work purposes away from their offices, such as virtual private network tunnels, but they impact the bandwidth for everyone. Company-owned devices can be pre-configured with security hardening features that offer the organization more advantages compared to employee-owned devices (Diogenes & Gilbert, 2015). Mobile device management solutions patch security and vulnerability gaps created by out-of-office use of mobile devices for work purposes through various mechanisms such as security patching and management directly from the hardware manufacturer or the operating system provider.

2.4 Mobile Device Management Features

Mobile device management solutions are primarily controlled by operating system providers and mobile device hardware manufacturers in terms of what the solutions can and cannot do on these devices through the utilization of application programming interfaces (APIs) (Hong et al., 2016). Therefore, mobile device management solutions can integrate these APIs to provide device management solutions. One of the features of mobile device management solutions is network segregation. Network segregation subdivides the corporate network into subnets (Arnaud & Wright, 2015). Each subnet is then assigned to a dedicated function and needs so that only authorized or certified entities can access the domains within those subnets, offering more secure connectivity within the corporate network. Therefore, data and other processes are inaccessible to internal and external unauthorized users.

Application management is another feature of mobile device management where a company can keep a catalog of company-owned application software that employees can access. These applications are securely and virtually managed and downloadable to employees in a restricted environment. They can easily be managed and updated with new security and functionality features.

Mobile device management solutions enable monitoring-related functionalities (Hayes et al., 2020). This is achieved through real-time network packet scanning of input and output requests. The company's information technology management can remotely perform functionalities on these devices, such as pushing logs, troubleshooting and correcting malfunctions, or locking and wiping the device's critical data in case of a security breach.

Policy enforcement is another feature of mobile device management. The company can enforce various corporate policies to manage devices, such as device-specific and platform-specific policies (Hayes et al., 2020). Device or platform-specific policies allow the advanced management of devices through their underlying operating system or platform providers. A personal policy is the second type that the company can enforce to govern the use of devices according to the corporate environment. Compliance policies are the third set of policies that govern the rules and regulations recommended by the company to be adhered to while using and managing these mobile devices.

Other standard mobile device management features include virtual private network configuration, predefined network settings, remote data wipes, device locking, remote disabling of native applications, whitelisting and blacklisting, data encryption enforcement, and device inventory monitoring.

Fig -1: Mobile Device Management

2.4 Mobile Device Management Elements

The mobile device ecosystem has profoundly evolved and will continue to evolve, and new challenges will keep emerging for corporates looking to integrate mobile devices into their computing infrastructure. Mobile device management solutions enable companies to address those challenges through several elements. Effectiveness is vital in mobile device management solutions because critical data and business operations are involved. One of the key elements is unified endpoint management. As discussed above, unified endpoint management involves devices that include Android and iOS platforms as well as other devices such as laptops and tablets running on other platforms such as Linux, macOS, and Windows. An effective mobile device management solution should enable a centralized

point of access to manage devices across all platforms and perform critical functionalities such as monitoring, remote data wiping, and remote device lock, among others (Ortbach et al., 2014). The solution should enable the management and sharing of data, device synchronization, and device support across all the platforms. Simplified security and support management is another critical element of an effective mobile device management solution. The solution should enable the company's information technology department to remotely access and manage mobile devices used by employees for critical business purposes. Productivity and efficiency are usually a company's primary goals when using mobile devices within their computing infrastructure (Ortbach et al., 2014). Management of these devices is vital in ensuring those goals are achieved. An effective mobile device management solution should allow the company to monitor device performance, troubleshoot problems, identify faults in time, push security updates, and ensure device operability in real time. Therefore, they can address issues to prevent disruption of core business operations and resolve them quickly to ensure the achievement of objectives.

Application installations, permission changes, and feature restrictions are critical functional processes in mobile devices onboarded onto the company's computing infrastructure. Additionally, blacklisting and whitelisting devices are inevitably crucial for the company. The mobile device management solution should enable the management of applications along with these crucial processes to ensure the successful implementation of mobile operations for business functions. It should also enable companies to host, manage, and distribute application catalogs for those devices within the company's computing infrastructure.

Security and access management policies enable a unified operational performance through employees' uniform device usage and management. They guide the use and access of corporate networks, enterprise apps, and other device features. They also define device and data security protocols that should be adhered to by all device users in the organization. All of these functions should be enabled by the mobile device management solution.

Some corporate entities look to convert their mobile devices into special-purpose entities. Retail companies, for instance, may want to turn their tablets into point-of-sale devices for an information entity. Other smart devices, such as smart televisions, may be turned into advertisement avenues. This element is called the lockdown feature (Collins et al., 2015). All these functionalities should be incorporated into a practical mobile device management solution.

Another practical mobile device management solution element is the over-the-air programming capability. This element forms the main component of enterprise-grade mobile device management solutions. It allows corporate information technology departments to perform remote mobile configuration of either a single device or the whole set of devices. Remote performance of functionalities such as remote device locking, remote data wiping, and remote software updates are made possible through this element.

2.5 Mobile Device Management Security

Security is a significant concern in mobile device management. Critical corporate data such as company customer records, database records, emails, documents, and enterprise applications are processed using these mobile devices. Security of this data is fundamental as it could determine the company's success or downfall. Mobile device management products are therefore built around the latest cryptographic techniques. They are built using the concept of containerization, where these critical data are processed within those containers (Jaramillo et al., 2013). Containerization ensures separating users' personal data from corporate data on mobile devices.

Documents are used every other time during corporate business operations and may contain critical corporate data that should be securely managed and used. Mobile device management can enforce restrictions on the inappropriate sharing of these documents to external domains or outside the corporate network domain (Kim et al., 2016). This will prevent misuse of the documents by the device users. Additionally, browsing and internet access are integral to remote device access and usage. Mobile device management can be used to force device users to use secure integrated browsers and restrict the use of native browsers, thus enhancing the security of data processed on the device and minimizing the risk of potential security breaches.

2.6 Mobile Device Management Implementation

In a typical setting, a mobile device management solution assumes the client-server architecture (Liu et al., 2010). They are administered using a client module and a server module. The server module may be located in data centers within the company premises or on a cloud platform. The server component sends commands and other resources to an agent module that resides on the mobile device's client component. The agent is configured in the end-user device and uses application programming interfaces (APIs) to communicate directly with the device's operating system. A single solution provider may provide both the client and the server modules, although some providers offer them separately.

The server module sends commands and policies directly to the client component through a management console. The client component automatically implements those commands and policies utilizing APIs to communicate with the client device's operating systems. Usually, the mobile device management software automatically identifies configured or connected devices and manages their processes and configurations to provide an easy-to-use environment for the information technology managers. The automation feature is crucial as it allows scalability. The server and client modules are configured according to the company's policies. During operation, a history of

connected devices is kept, and settings and configurations are automatically pushed over the air to the unconfigured devices.

Over time, mobile device management solutions have evolved to become more efficient. Previously, the mobile device needed a connection or a sim installation to enable configuration and settings. After that, the client had to initiate the updating or configuring process to enable the manager to push logs and updates onto the device. This was a cumbersome process and undermined scalability and efficiency, especially where many devices were involved. The current solutions are entirely automated through the use of application programming interfaces.

2.7 Importance of Mobile Device Management

The two major concerns about mobility in the company are efficiency and security. The primary reason for adopting mobile device usage in corporate entities is to improve efficiency for employees by allowing the mobile and remote performance of business processes through those devices. However, the increase in the number of mobile devices connected to the company's computing infrastructure presents more security risks and vulnerabilities. These devices store and process much company data and are, therefore, targets for malware attacks and security breaches. For these reasons, companies need mobile device management to address the concerns.

Mobile device management facilitates the company's ability to manage and secure devices remotely. It enables companies to deliver critical security configurations and other applications to the devices to not only support employees' ability to improve their performance and efficiency but also ensure security across the resources. The importance of mobile device management has been elevated by the massive deployment of enterprise applications to mobile devices requiring protection and management solutions, vulnerabilities associated with employee mobile device usage, and ensuring uniformity and standardization of device usage within the organization.

2.8 Mobile Device Management Landscape Overview

The mobile device management industry was introduced in the early 2000s and has since evolved in various dimensions. In the early stages, the focus was mainly on enterprise mobility. However, the industry improved over time due to the volatile and ever-evolving industry. Mobile device management solutions evolved into unified endpoint management (UEM) solutions to accommodate the need to support different devices operating on different platforms, thanks to the bring-your-own-device policy implementation (Yamin & Katt, 2019). On-premises solutions were also used in the early stages before cloud computing gained traction and reshaped enterprise computing. Mobile device management solutions have recently been primarily offered through the cloud due to their flexibility and the pay-as-you-go model that many organizations prefer.

2.9 Advantages of Mobile Device Management

Mobile device management offers several advantages to corporate entities. The most significant advantage is the automation of repetitive and large-scale tasks. Device management automation saves much time and increases efficiency. Manual configuration of devices can be cumbersome, especially if it involves a large group of devices. Mobile device management allows the company to configure and manage multiple devices simultaneously, making it easier and saving time.

Additionally, mobile device management helps increase employees' productivity and efficiency. Essential applications and services can be forcefully allowed on devices during work hours to eliminate distractions caused by applications such as social media. Employees will therefore be prevented from wandering away from important business activities on the device, allowing them to give more attention to their work, thus improving performance and efficiency.

Regulations can be pain points for organizations. They must comply for various reasons, including personal data processing and storage. Mobile device management ensures compliance with these regulations by allowing companies to deploy compliant configurations and resources to mobile devices remotely. The increasing complexity of cyber-attacks and security threats gives organizations little room to choose between implementing mobile device management solutions or not. Security is costly; therefore, the company needs solutions that enable them to have secure operations on mobile devices, and mobile device management allows them to achieve it.

3. Mobile Device Management Industry Overview

According to Fortune Business Insights (2020), the mobile device management industry had a market value of USD 3.97 billion. It is anticipated to grow from USD 4.75 billion in 2022 to USD 211.3 billion by 2029. The market growth between 2019 and 2020 was marked at 14.9%. The key driving force behind the industry's growth is the advancement of personal equipment with better capabilities than company-owned devices. The restraining factor is the high cost of implementation in smaller organizations and the increasing security concerns. Mobile device management industry segmentation includes deployment, organization size, region, and end-user. The market is segmented into cloud-based and on-premises, with cloud solutions having the larger market share due to their scalability and flexibility. Enterprise size segmentation has seen large enterprises take the largest market share in 2021. The end-user segmentation categorizes the industry into IT and telecommunication, government, retail, healthcare, BFSI, and others. The healthcare category's most significant market share is

attributed to the high-value data it processes. Regional segmentation divides the industry into South America, Europe, North

America, Asia Pacific, and the Middle East and Africa. The key industry players include VMware Inc, IBM Corporation, Microsoft Corporation, Soti Inc, Scalefusion, and Cytrix Systems Inc.

Table -1: Mobile device management industry segmentation

Segment by	Entities
Deployment	Cloud-based, On-premises
Organization Size	Large organizations, Small and Medium Enterprises
End-user	IT and Telecommunication, Government, Retail, Healthcare, BFSI, and others
Region	South America, Europe, North America, The Asia Pacific, and The Middle East and Africa

3. CONCLUSIONS

Mobile device management offers crucial business support features for companies that use mobile devices in their operations, both company-owned and employee-owned devices. Mobile device management enables organizations to remotely and effectively manage mobile devices signed into their network. With the rise in the adoption of mobile devices in company operations, security threats have increased as these devices have become malware targets. Companies are therefore mandated to take responsibility for securing their vital data being processed and stored on these devices through mobile device management solutions. The solutions have evolved to address issues and challenges that have come up, such as diverse platforms. Different solutions have been created to cater to different organizational needs. However, there are core elements that each mobile device management solution must have to be deemed effective. Mobile device management offers many advantages to companies, especially in terms of security and automation. Mobile device management is a critical technology resource that companies can utilize to improve efficiency and productivity while allowing the simplicity of operations in a secure and regulations-compliant manner.

REFERENCES

[1] Afreen, R. (2014). Bring your own device (BYOD) in higher education: Opportunities and challenges. International Journal of Emerging Trends & Technology in Computer Science, 3(1), 233–236.

[2] Arnaud, J., & Wright, J. W. (2015, March). Network segregation in the digital substation. In 13th International Conference on Development in Power System Protection 2016 (DPSP) (pp. 1–4). IET.

[3] Collins, L., Collins, L., & Ellis, S. R. (2015). Mobile Device Management (MDM). Mobile Devices: Tools and Technologies, edited by Lauren Collins, and Scott R. Ellis, pp. 297– 312.

[4] K. Diogenes, Y., & Gilbert, J. (2015). Enterprise Mobility Suite Managing BYOD and Company-Owned Devices. Microsoft Press.

[5] Fortune Business Insights. (2020, July). Mobile Device Management Market Size, Growth | Share by 2028. https://www.fortunebusinessinsights.com/mobile-device-management-market-106381.

[6] Hayes, D., Cappa, F., & Le-Khac, N. A. (2020). An effective approach to mobile device management: Security and privacy issues associated with mobile applications. Digital Business, 1(1), 100001.

[7] Hong, S., Baykov, R., Xu, L., Nadimpalli, S., & Gu, G. (2016, February). Towards SDN-Defined Programmable BYOD (Bring Your Own Device) Security. In NDSS.

[8] Jaramillo, D., Katz, N., Bodin, B., Tworek, W., Smart, R., & Cook, T. (2013). Cooperative solutions for bring-your-own-device (BYOD). IBM journal of research and development, 57(6), 5-1.

[9] Kim, G., Jeon, Y., & Kim, J. (2016, October). Secure mobile device management based on domain separation. In 2016 International Conference on Information and Communication Technology Convergence (ICTC) (pp. 918–920). IEEE.

[10] Liu, L., Moulic, R., & Shea, D. (2010, November). Cloud service portal for mobile device management. In 2010 IEEE 7th International Conference on E-Business Engineering (pp. 474–478). IEEE.

[11] Ortbach, K., Brockmann, T., & Stieglitz, S. (2014). Drivers for the adoption of mobile device management in organizations.

[12] Steiner, P. (2014). Going beyond mobile device management. Computer Fraud & Security, 2014(4), 19–20.

[13] Tairov, I. (2019). Mobile device management as a component of corporate IT infrastructure.

[14] Yamin, M. M., & Katt, B. (2019, January). Mobile device management (MDM) technologies,

[15] Issues, and challenges. In Proceedings of the 3rd International Conference on Cryptography, Security, and Privacy (pp. 143–147).

BIOGRAPHIES

I am currently pursuing my Master's in cybersecurity & networks from the University of New Haven in Connecticut. I have already done my MBA in HR and bachelor's in computer science. I have 10 years of experience in IT infrastructure and has been an entrepreneur for 6 years.