ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 7, Issue 2, pp: (96-98), Month: April - June 2019, Available at: www.researchpublish.com

A Review on MDM Solutions

[1]Sujayeendra Boodur, [2]Vanshika Kuchhal, [3]Mohammad Saif Sabir, [4]Divyanshi Gupta

[1]Dept. of Information Science, [2]Dept. of Computer Science, [3]Dept. of Computer Science, [4]Dept. of Computer Science,
[1,2,3,4] R.V College of Engineering, Bengaluru, Karnataka, India

***Abstract*: Mobile Device Management (MDM) solutions allow organizations to manage and secure the corporate devices from a single dashboard, where these devices are overseen remotely by the administration. The essential need for corporate IT security is the protection of organization information. This is principally done by MDM solutions which manage corporate information isolation. This paper gives a survey on various MDM solutions and a discussion is made on their major characteristics.**

***Keywords*: MDM, UEM, BYOD, Azure, Trusted Platform Module, LDAP, (HTTPS/SSL), Open SSL, ACC.**

I. INTRODUCTION

As the bring your very own device (BYOD) approach turns out to be progressively prevalent across numerous enterprises,Mobile Device Management solutions are important venture apparatuses. They enable employees to have prompt access to the internal resources and assets. The variety of versatile mobile platforms, working frameworks and versions can make management of these devices difficult. Mobile device management provides the solution and gives a rich answer for security concerns and availability inherent to enterprise mobility. Primarily it involves managing large scale deployment of mobile devices from a single console. Also enrol devices in the enterprise rapidly and effectively, arrange and update device settings over the air and authorise security consistent policies. Finally, provide secure device access to corporate assets. Through this paper, we give a review of top MDM solutions currently available in the market. We look into various functionalities provided by different MDM solutions and infer their advantages and limitations present if any.

II. DIFFERENT MDM SOLUTIONS

In [1], various functionalities of Microsoft Intune MDM are depicted. This solution uses Azure Active Directory (Azure AD) for user authentication and sign-on (SSO) experience. The system uses BitLocker to provide data encryption which itself uses Trusted Platform Module (TPM) to lock the encryption keys that protect the data. The solution also provides remote device wiping functionality which can wipe all MDM policies enforced on the device and reset the operating system to its default state. The solution also provides various security measures in terms of new application installation, execution and removal by restricting the functionalities of the app, the resources it uses and enforcing pin access to company applications.

In [2], various functionalities of MaaS360 MDM is depicted. This solution uses a cloud extender which receives sign in credentials from MaaS360 cloud and provides Lightweight Directory Access Protocol (LDAP) authentication. Data encryption for application data is done via AES-256 CTR encryption algorithms. Data encryption in Android is done by using SQLCipher with the OpenSSL (AES-256) FIPS 140-2 compliant crypto modules. Data encryption in iOS uses the built-in CommonCrypto FIPS 140-2 compliant encryption. Remote wipe and Selective wipe features are provided to restore device to factory settings and remove corporate data from device respectively. Various security measures such as enforcing security policies and access controls which restricts apps to run only on approved devices, app tunnelling to securely connect app to corporate networks, app configuration and single sign on are provided to protect devices from new applications to be installed.

With the capacity to adjust to the changing environment of network of mobile phones, Cisco Meraki as given in [3], offers numerous solutions which incorporate mobile application development, mobile content, management, mobile device management and mobile identity management solutions. Clients can sign on using credentials made in the Meraki-

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 7, Issue 2, pp: (96-98), Month: April - June 2019, Available at: www.researchpublish.com

facilitated server either through splash or by means of WPA2. Meraki APs should reach the Meraki cloud so as to use the Meraki-hosted authentication server. To prevent the unauthorised reading, replicating, adjustment or erasure of Customer Data.Encrypted communication between Meraki equipment devices and Meraki's servers (HTTPS/SSL), is ensured just as between Meraki's servers.Logging of activity of admin (time, IP, and estimated location of signed in administratives) and account passwords are all encrypted on Meraki servers. Cisco Meraki provides Selective Wipe feature which removes everything previously pushed to the device through the Cisco Meraki Systems Manager dashboard, including documents, apps and configuration profiles. The two profiles and managed applications can be removed from Cisco Meraki Systems Manager customer devices remotely by means of dashboard. In the event that an application or profile must be removed from ALL managed devices, there are two methods: temporary and permanent. In the event that the application was installed manually, or through other means, it won't be possible to remove it remotely from systems manager.

Various unique features of VMware's AirWatch are depicted in [4]. For User Authentication, VMware Identity Manager provide its own identity provider which is programmed to align with AirWatch Cloud Connector (ACC) and in-built Kerberos authentication. The Encryption and Decryption methods used to work on raw data is defined in AirWatch AW Controller. The AirWatch's SDK provides basic encryption and decryption on raw data for iOS that system encrypts and decrypts with the help of SDK's internal encryption/decryption keys. AirWatch App Wrapping is used for Android OS. Wiping the device data remotely is an important feature by AirWatch mdm used to protect important corporate data in case of stolen or lost device. Wiping the data generates logs, which could be reviewed later by the administrator. A unique feature of defining a wipe threshold is provided which specifies minimum number of devices that could be wiped in certain amount of time. AirWatch uses Reputation Cloud Service to check applications with the Reputation Analysis on applications for Android devices. The results of the analysis are then used to decide to either deploy or remove applications from the device for security.

III. INFERENCE

Based on the detailed study of the various Mobile Device Management solutions we summarize some of the majorly used solutions in the market. A comparative study of some of these competitive products are given in the table below:

TABLE I: A COMPARISON OF MDM SOLUTIONS

	Microsoft Intune	**IBM MaaS360**	**Cisco Meraki**	**Vmware AirWatch**
Features	- Device Enrolment - Device Compliance - Device Management - Conditional Access Settings - User Roles Controls	- Remote App Management - Interactive App Catalogue - Multitenant Architecture - Simple Device Enrolment	- Tagging Mobile Devices -Analyze Network Activity - Remotely Deploy Apps - Enterprise Connectivity	- Single admin console - Multitenant Architecture - Remote TroubleShoot - Data mart Integration
Pricing	*****	****	Quote basis	***
Language Support	- English - German - Hindi - Japanese - Russian and various others	- English - Polish	- English	- English - Turkish - Dutch
Integration	- Office 365 - Azure	- Bluemix - Office 365	- OneLogin	none

	- Microsoft Graph API	- Cisco Identity Services Engine		
Non-Supportable Devices	- Linux	- Linux	- Linux - Windows Mobile	- Windows - Windows-Mobile - Mac - Linux
Clients	- Avanade	- Flipkart - OpalStaff - Bancroft	- Grab - Infors-HT	- Lufthansa -GlaxoSmithKline

*- depicts the unit of pricing

The user experience for any kind of MDM solution stands at the utmost priority. Right from easy and simple enrollment of devices till the protective support of the enterprise data, these solutions are continuously gaining the client and the market support. Among these given solutions, VMware AirWatch and IBM MaaS360 have a multitenant architecture which helps in optimal utilization of resources with the consistency in the system.This also makes the troubleshooting easier.

With the multi-language support for its various clients as mentioned in [5], Microsoft Intune is the only one in the group of above solutions which supports Unix/Linux based servers and mobile devices all in the central portal. As the market grows, Cisco Meraki is the reasonable solution for the various organizations. One of its salient features is the tagging of mobile devices which helps system administrators to determine appropriate security policies for a particular section of users.

IV. CONCLUSION

Mobile Device Management isn't just about purchasing the most recent cell phones or putting email on a worker's telephone. It's tied in with changing your business with secure portability that enables enterprise employees to be beneficial and effective wherever they work. When it comes to mobile expense management, VMware AirWatch and IBM MaaS360 stand out with the most efficient management. Also IBM MaaS360 provides the support for Blackberry devices and provides the data to the admin for the recommendations based on the analytics of the provided data which is not given by any one mentioned in the list above. Combined with VMware's Workforce One management platform, this blend gives clients all that they need to manage, track and grow a quick changing device portfolio.IBM MaaS360 keeps up its remaining in our second take a gander at this item. While its cost has descended marginally, regardless it has a shortcoming contrasted with the challenge while overseeing Windows Mobile gadgets. Yet, it works positively outside of that moderately minor ding. Microsoft Intune is amongst the best device management choices for people running Microsoft-driven conditions. The pack alternatives with Azure-based character and security instruments have developed and speak to a ground-breaking development way. Nonetheless, the cost will be generous and, for those running non-Microsoft stages, there are some disregarded highlights, as well.

REFERENCES

[1] Microsoft. (2018,March) “Microsoft Intune Privacy and Data Protection Overview”. Microsoft Intune. [Online]Available:Windows Intune Privacy and Data Protection Overview - Microsoft ...download.microsoft.com/.../c/.../intune_privacy_and_data_protection_overview.pdf

[2] IBM. (2015,February) “IBM MaaS360 with Watson Unified Endpoint Management”. IBM MaaS360. [Online] Not Available

[3] Cisco. (2016, December).”Cloud Managed IT for modern Organization”.Cisco Meraki . San Francisco. [Online]. Available: https://meraki.cisco.com/lib/pdf/meraki_whitepaper_fullstack

[4] VMware. (2017,June). “VMware AirWatch Installation Guide”. VMware AirWatch. [Online].Available:https://docs.vmware.com/en/VMware-AirWatch/9.1/VMware%20AirWatch%20Installation%20Guide%20v9_1.pdf