The Road to Unified Endpoint Management (UEM)

East Carolina University

ICTN-6875: Emerging Technology

Dr. Phil Lunsford

14 July 2019

Abstract

It can be argued that today's society not only thieves but is also more efficient due in part to mobile technology. As with all technology, mobile technology came with vulnerabilities that malfeasant individuals were keen to exploit. The use of personal mobile devices flourished in the mid-2000s with the release of the Apple iPhone and subsequent Android devices. Businesses soon learned the benefits of a Bring Your Own Device (BYOD) program. It soon became an almost overwhelming task to manage personal devices that were not controlled by the Information Technology (IT) department, yet allowed access to organizational resources. As technology advanced, the only constant seemed to be that of managing and securing the new technology which became more and more complex. As IT management grew in efficiency, the scope of control was expanded to not only mobile technology but all technology under a single umbrella. This paper will discuss how Unified Endpoint Management (UEM) was the culmination of, and a natural progression from other management systems. As advancements in technology thrived, so did business in the incorporation and implementation of technology transitioning from one management system to another. BYOD programs highlighted the need to develop what became Mobile Device Management (MDM). MDM then progressed to Enterprise Mobility Management (EMM) which then expanded to UEM. Like the Darwin theory, this paper will show how management systems have evolved to keep pace with the evolution of technology and security requirements. Along with the evolution of technology is the ever-increasing manner in which technology is incorporated into everyday life. It is a fine line between usability and security. Management leans towards security where the user demands usability. UEM provides a balance of what is required along with what is desired.

Table of Content

Introduction

As far back as the 1990s personal electronic devices existed in the work place. Of course, back then, it was limited to only the upper echelons of management. This was due in part to the cost and viable applications for the everyday employee. As personal devices dropped in price and technologies in the personal cellular phones advanced, more and more devices started appearing at the work place. At this point there still was no concern for alarm because none of these devices had access to organizational resources. All that changed with the introduction of the first Apple iPhone. Now there was an affordable personal device that could access email servers as well as wireless networks. Unbeknownst to the technology industry at the time, this is where the path to Unified Endpoint Management (UEM) began. This paper will show how in the beginning, the primary focus was on how employers could benefit from employees-using their own devices not funded by the organization. We know now, having unmonitored, possibly corrupted devices accessing a secure environment is a huge security vulnerability. Out of this scenario came Bring Your Own Device (BYOD). BYOD was not a technology but a series of policies and procedures designed to control the access of personal devices in the workplace. Proving insufficient in protecting sensitive information and other network resources, Mobile Device Management (MDM) was introduced. MDM was a technology that allowed security professionals to monitor, update and even remotely wipe clean when needed. As technology advanced so did the need to update the management systems. MDM would be replaced with Enterprise Mobility Management (EMM). EMM would eventually be replaced by Unified Endpoint Management (UEM). This paper will show how as technology progressed, so did management systems resulting in the widely used technology of UEM. Also discussed is how the

robust nature and complexity of UEM is a result of lessons learned by the management systems that came before.

In the Beginning

It all started around 2007 with the release of the first Apple iPhone. Then, other smart phones with unprecedented capabilities were introduced. This was followed by the iPad and the Tablet. Smart devices that enabled an individual to take their computing needs with them anywhere they went. It was not long before they appeared at the workplace. First for personal use and then for accessing resources provided by their employer. There was a noticeable increase to employee satisfaction and productivity; unfortunately, it was not all pros without cons. What seems obvious to the Information Technology (IT) professional today, was not so obvious or at least as concerning in 2009. Multiple platforms operating on multiple Operating Systems (OS) were accessing organizational resources unchecked and unmonitored. As one could imagine, this caused a lot of security issues. Another problem, employees were authorized to use their personal devices for conducting work related activities on personal devices. This allowed employees to work away from their established work space. In some cases, employees worked without pay and in other cases employees racked up overtime hours that were not previously authorized. Either way it is easy to see how legal issue mounted. The list of benefits and vulnerabilities is well documented, but what is apparent is that the benefits outweighed the risk, "Every employee can benefit from the increased productivity, flexibility, and efficiency that mobility offers" (Information Management, 2015). The term Bring Your Own Devices (BYOD) appeared in 2009. One reason the BYOD term came about was to describe activities taken by employees upon realizing the capabilities of devices now available. The other reason was out of necessity as

mangers look for a way to embrace but control this growing phenomenon. Management and Security realized the importance of a good BYOD program.

Bring Your Own Device (BYOD)

BYOD is a term that is thrown around a lot and even though the acronym means the same in every case, the meaning behind the term does not. For instance, BYOD can describe the process whereby employees are allowed to bring personal devices to the work place for the purpose of conducting work-oriented activities. On the other hand, BYOD can also refer to the business strategy that governs the use of personnel devices in a business environment. In the context of this paper, the latter will be used. The use of personnel devices was an innovative concept that developed on its own as employees took it upon themselves to bring devices in as a way to make their job easier. Initial pushback by management was soon reversed as the benefits stemming from this development became apparent. Bringing your own device went from being against the rules to being supported and even encouraged. Now that management was onboard, a mechanism to control this was needed. In order to verify the security profile, monitor and, to some extent control the devices, a program needed to be developed. Here is where BYOD the management system comes into play. The new BYOD program would establish the policies and procedures necessary to ensure the integrity and security of organizational data, resources and infrastructure.

To establish an effective BYOD program, the policies that will govern the program must first be written. Listed below is an example of policies possibly needed based on the business environment. Acceptable Use: This will explain the parameters of how a device will be used when connected to the organizational resources. This must be a clear and concise document not open for interpretation.

- Acceptable Product List (APL): Due to the complexity of allowing every make and model device on the market, it is wise to limit the supported devices to a manageable number.
- Compliance: Compliance refers to any and all regulations in place to protect the integrity of the data, and its collection. Due to federal, state and other regulation such as the Health Insurance Probability and Accountability Act (HIPAA) it is important that every employee with access understands these policies.
- Applications: Applications or Apps have almost become a necessity in today's society. This policy should specify which applications will be authorized for use.
- Privacy: To ease the mind of employees a policy that ensures their privacy should be written. This document should provide the employee no doubt that their privacy will be respected.
- Security: Probably the most important area, security should be a series of policies that protect the organization, its resources and yes, the employee.

By no means is this a comprehensive list of areas needing to be covered, but rather an idea of the complexity and variety of needed policies. "There is no right BYOD policy." (IBM Security, 2016).

It was during the development of the BYOD the program, that the foundation of future management systems, and what areas needed to be addressed, would be outlined. At no time is any program thought to be complete. Even now as technology advances, so do the programs designed to manage and control the environment for which they were designed. Written policies and procedures are controls for employees and the use of systems. What can be done to control devices for instance if a device is lost, stolen or compromised?

Mobile Device Management (MDM)

From written policies and procedures to configured policies installed on individual devices, polices for a computer is just a configuration setting that controls what the device can and cannot do. When dealing with a device that is not physically connected to the network, policies need to be pushed to the device Over-the-Air (OTA). To effectively push, install, run and monitor these policies, a different management system is needed. “Mobile device management (MDM) is software that allows IT administrators to control, secure and enforce policies on smartphones, tablets and other endpoints” (Rouse, 2017). MDM does more than push and enforce policy. An MDM system is very complex and tailored to the organization for which it is designed. Because of the complexity and cost, not all MDM systems are the same. Almost everyone travels with their electronic devices. Should these same devices be used at their place of business? What can a business do to safeguard sensitive data and applications stored on that device? MDM would allow an organization’s administrators to remotely wipe a device in case the device was lost or stolen. If an employee was terminated, MDM administrators could wipe the organizational data without compromising personal data. Another feature of an MDM system is the ability to control access based on location and or time. This would ensure that resources are not available when the employee or nefarious agent should not be accessing them. Although MDM was originally developed with the need for controlling hardware, since its inception MDM has grown to do so much more. For instance, MDM provides services such as mobile application management, profile management, mobile content management, asset management, audits and reports, and even enrollment. “The intent of MDM is to optimize the functionality and security of mobile devices within the enterprise while simultaneously protecting the corporate network” (Rouse, 2017)

Enterprise Mobility Management (EMM)

MDM is a robust system that enables enterprise administrators to control mobile devices. Advancements in technology have created capabilities and subsequent vulnerabilities. These advancements often render the MDM system incapable of meeting requirements in some of the more robust enterprises. Part of the problem was that MDM was designed to manage the devices and protect the network. Technology now needs more. EMM not only manages devices and secures the enterprise it also enables devices on a broader level then previously able. The actual definition of EMM is constantly changing as do the EMM systems themselves. "The EMM market is evolving to provide ever more comprehensive (and specific) services for device and application management." (Kapko, 2017). Implementing an EMM solution is not only costly and invasive, an EMM solution is not always needed. Since the first mobile device was introduced into and enterprise environment, corporations have been amassing information and establishing a robust knowledge base. There are entire companies that specialize in the analysis and development of EMM systems. Hiring a consultant is often advisable to determine if an EMM system is needed and then design the EMM system if that is the desired course of action. "While it can manifest itself in various ways, it generally consists of a suite of mobile management systems and services that protect intellectual property; specific processes that ensure the security of data; and systems that must integrate with a wide range of enterprise IT systems to meet a range of corporate concerns." (Kapko, 2017). Although the EMM systems does not completely replace the MDM systems, EMM is more complex and capable. "The EMM platform has the potential to affect every employee, so treating it as mission-critical is crucial." (David & Clark, 2018). Just as fast as EMM superseded MDM, so will EMM be superseded.

Unified Endpoint Management (UEM)

"Unified endpoint management (UEM) is an approach to securing and controlling desktop computers, laptops, smartphones and tablets in a connected, cohesive manner from a single console." (Rouse, 2016). Wireless and cellular communications have allowed for the use of electronic devices just about anywhere you go. Whereas before mobility, concern was primarily with mobile phones, tablets and iPads. Now administrators need to be concerned with laptop and desktop computers as well. Also, some organizations have transitioned to wireless communications and network connectivity even within the confines of their office space. This can be partially attributed to the cost of hardened infrastructures and the flexibility and freedom to roam that wireless offers. "Enterprise mobility management is transitioning to unified endpoint management, as administrators use EMM to support a broad range of device platforms, including iOS, Android, Windows 10, macOS and EMM-manageable IoT devices,". (Kapko, 2017). With UEM you get single-pane management software and internet of things (IoT) management. Single-pane management takes the array of devices and puts them into one management system. IoT is growing and gaining control of IoT devices is crucial. According to Anna Kungsdahl there are seven best practices for UEM. These best practices are.

1. Start with the user.
2. Adopt a cross-functional approach.
3. Implement cross-platform solution, with a single pane-of-glass for visualizing technology assets and consumption in datacenters, cloud, mobile, and desktop.
4. Embed security in the request process and consumption of technology assets.
5. Ensure a basic level of security on all devices and provide support for additional levels of security for select groups and devices.
6. Automate processes to lower the total cost of ownership.
7. Address UEM as a continuous process.

Note: Diagram comes from (Kungsdahl, 2018)

Every company may not need a UEM solution but for those that do, the management that proceeded UEM will just not do. "UEM solutions manage security, operating systems, patches,

applications, and hardware for you, and they reduce the complexity of ever-expanding device diversity." (Hess, 2017)

Summary

The road to UEM, unbeknownst to everyone, started with the first iPhone. Smart devices inundated the market and it was not long before employees discovered ways to tie into their employers' network to make their life easier. In the begging a comprehensive BYOD program provided the employees the responsible parameters for using personal devices in a business environment. Technology grew as did the capabilities of smart devices. This created a new management need spurring the MDM system to work in conjunction with BYOD. Technology and innovation outgrew MDM requiring yet another management system with more capabilities which resulted in EMM. UEM came about through the need for an even more robust management system and all the lessons learned from its predecessors. Since UEM is an evolving system, speculations are that it will be around for a long time.

References

David, M., & Clark, K. (2018, January). Learn what an EMM platform can achieve in the enterprise. Retrieved from https://searchmobilecomputing.techtarget.com /feature/The-capabilities-and-challenges-of-an-EMM-platform

Hein, D. (2019, July 12). Unified Endpoint Management (UEM): The Basics and Benefits. Retrieved from https://solutionsreview.com/mobile-device-management/unified-endpoint-management-uem-the-basics-and-benefits/

Hess, K. (2017). Unified Endpoint Management for Dummies. Retrieved from https://searchmobilecomputing.techtarget.com/UEM/document/1524763460_415

IBM Security. "The Ten Commandments of bring your own device (BYOD)." IBM.com. 12 Aug. 2016. Web. 21 Nov. 2016.

Kapko, M. (2017, October 09). What is EMM? Enterprise Mobility Management explained. Retrieved from https://www.computerworld.com/article/3230510/mobile-device-management/what-is-enterprise-mobility-management-emm.html

Kungsdahl, A. (2018, June 16). UNIFIED ENDPOINT MANAGEMENT (UEM) – SEVEN BEST PRACTICES. Retrieved from https://www.snowsoftware.com/int/blog/2018/06/16 /unified-endpoint-management-uem-seven-best-practices

Laird, J. (2014, November 7). A Brief History of BYOD and Why it Doesn't Actually Exist Anymore. From http://www.lifehacker.co.uk/2014/11/07/brief-history-byod-doesnt-actually-exist-anymore

Moyer, J. E. (2013, July 15). Managing Mobile Devices in Hospitals: A Literature Review of BYOD Policies and Usage. from http://www.tandfonline.com/doi/abs/10.1080/ 15323269.2013.798768

Rouse, M. (2017, November). What is mobile device management (MDM)? - Definition from WhatIs.com., Retrieved from https://searchmobilecomputing.techtarget.com/definition/mobile-device-management

Rouse, M. (2016, October). What is unified endpoint management (UEM)? - Definition from WhatIs.com. Retrieved from https://searchenterprisedesktop.techtarget.com/definition/unified-endpoint-management-UEM

10 smart strategies for BYOD success. (2015). *Information Management, 49*(6), 19. Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/1734164346?accountid=10639