IBM Security
Thought Leadership White Paper

Enterprise Mobility Management

The Big Bang Theory – how Mobile Device Management exploded to include devices, apps and content

IBM

Introduction

The boundaries between working "in the office," "on the road," or "at home" have been blurred by the untethered power of smartphones, tablets, and other portable devices. Employees expect the flexibility to work on the devices they choose, and employers have come to expect always-on availability. That business requirement often conflicts with those in charge of securing corporate networks and data. In some organizations, this has led to the draconian answer "no." But today those responses are few and far between. The norm today is, "It depends." One also can't forget the microcosm of different departments within an organization, which yet again causes great debate on how much access is needed, balanced against how to protect sensitive data.

To help maximize mobility, a nuanced strategy is the order of the day. For mobility's transformative potential to be realized, IT needs to become a business partner that understands business drivers and then devises the technology roadmap to support everyone's goals.

The universe of mobility is a complex thing, and it is ever-expanding – much like our actual universe. The other similarity mobility shares with our ever-expanding cosmos is the potential that can be realized through a rational, analytic, and extensive understanding.

The mobility explosion: The big bang that keeps expanding

At first there was darkness, especially for those who needed to get work done on the road or at home. Workers left their data and productivity programs on their cumbersome desktops. Laptops made it possible to work outside the office, but connectivity was costly and inconsistent. Also, the minute you closed your laptop, you entered an information black hole of nothingness.

With the arrival of BlackBerry, people in corporate leadership became connected to their office. There was light, but it was more like faraway stars in a dark night sky than a beacon of brightness.

Then, in a white-hot burst of innovation, came the first smartphone.

The light spread, as did the devices, to people virtually everywhere. Executives had BlackBerries, but suddenly new touch-based devices with iOS and Android operating systems started to enter people's pockets and their workplace.

Then – another bang – the tablet arrived, with larger screens that enabled even more work and play. Their larger size and increased intelligence finally made data retrieval and manipulation on the move a reality. The workers became enlightened, but IT remained somewhat in the shadows, unconvinced. What devices should connect to corporate resources? Which should not? What was safe?

Managing the big bang of mobility

How could the big bang of mobility be managed?

Managing devices

Enter Mobile Device Management (MDM), the nucleus of IT's Big Bang point solution for being able to gain visibility and apply some controls. In this universal expansion, MDM gave IT the ability to enforce a passcode, connect to corporate resources such as email and Wi-Fi networks, and monitor devices.

Through APIs built into the operating system, IT could configure settings, enable or disable features, locate and lock devices remotely and even partially or fully wipe data when necessary.

Devices managed by external service providers estimated to grow over 50 percent in 2015 [1]

IT declared this to be good, and the people mostly agreed. But as users and apps became more sophisticated, and documents such as spreadsheets and Word docs became manipulable on mobile devices, many companies found they needed more than just MDM.

In response to this plea, there came another expansion – the advent of solutions for app and content management and the separation of work and personal in the form of containers.

Managing apps

Mobile Application Management (MAM), as the name implies, focused on the lifecycle aspects such as distribution, updates, enterprise app catalogs, blacklisting/whitelisting, and security. MAM was needed to manage the exploding universe of public and custom apps.

But applications are not "one size fits all"– some are not written or owned by the enterprise – so the ability to control them would always be limited. One ideal application for MAM is controlling a device dedicated to a single app in what has sometimes been dubbed "Kiosk Mode." Use cases in retail stores and hotels have enabled this mode to expedite the check-in process, look up inventory, or order food and beverages.

Managing content

Again, the universe expanded. In a burst of light the people were given Mobile Content Management (MCM). Now, files and documents could be shared selectively with the right members of a team. Some people have permission to see some documents, forward them, but not others. Some can edit the documents and save their changes back to the file share for all to see and sync them across their devices. MCM brought this kind of enablement and control to enterprise mobility. The future also held hope and promise – the potential for secure, private, simultaneous collaborative editing of shared documents on mobile devices without worry of colliding into rocky security asteroids often found with public file share services.

"But we want to show co-workers pictures of family and pets and we want to check work emails before work in the morning!" the people said. "Can't we do both on one device?"

This series of expansions, in such a short period of time, left the organizations with such a dizzying array of choices to manage mobility, that IT quite nearly plunged into self-imposed darkness once again, lest it attempt to make sense of the endpoint management options now available.

66 percent of IT Managers' greatest security concerns stem from connecting personal devices to the corporate network[2]

Boundaries between work and life

Another flash – many of the people were now prepared for this burst of light and had bought sunglasses. From the sky dropped a container, sharpening the focus of MAM and MCM, and creating a dual persona experience.

A container offers a more fine-grained approach to managing both apps and content based on context and identity – who they are, where they are located, and what role they have in the organization. It also separates personal and enterprise data by shielding enterprise apps from personal apps and sandboxing work email or documents.

Containers protect employee privacy and provide separate controls for company use, such as network access and secure, company-approved web browsing. They can prevent copying data from one "side" of the device to the other, and the employer-owned container can be wiped or locked if nefarious activity occurs, without affecting the other "side" of the device. The archetypal use case is an employee in a highly regulated industry entrusted with sensitive company information.

Enterprise Mobility Management: For today's mobile universe, and what's next

IT was overjoyed. Now the people could download apps from commercial app stores without compromising company systems. Containers also gave people more flexibility, as the "work side" of the container could simply be deleted, without affecting the rest of the data and apps on the device.

Many enterprises use multiple software platforms and exchange numerous document types constantly on desktop computers and local networks. "Why can't we do this securely on our mobile devices?" the people asked.

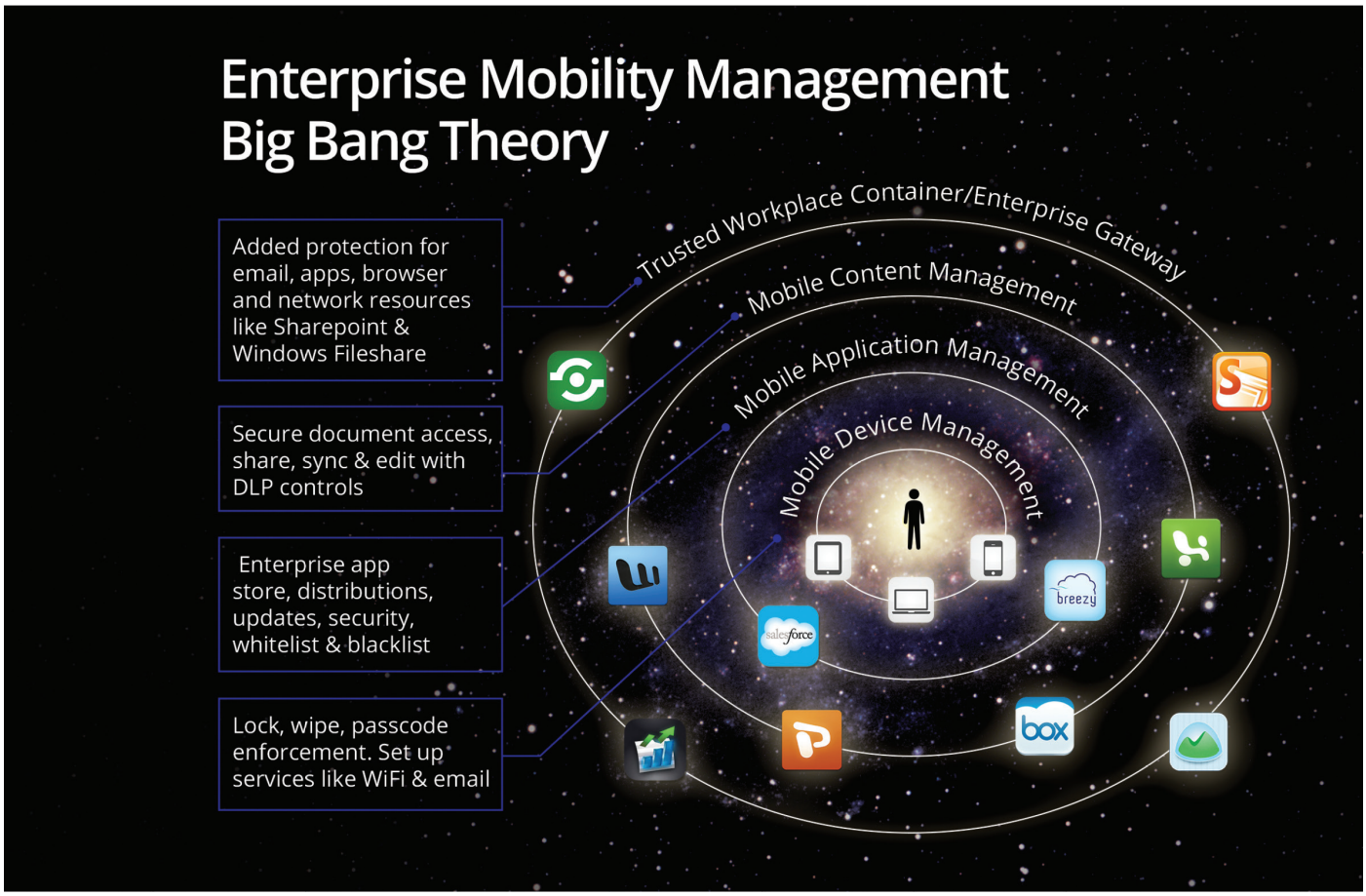

Figure 1: Enterprise Mobility Management Big Bang Theory

28 percent of CIOs said that their organizations do not have a mobile technology strategy[3]

Organizations are undergoings undergoing another cataclysm, but this time it is more like an implosion than an expansion. Many of the point solutions that solved aspects of mobile business problems are being consolidated under Enterprise Mobility Management (EMM), which enables IT to easily put its arms around the entirety of data and security concerns in the mobile universe. Today's epoch is like a Renaissance from the Dark Ages and promises to offer more choices to organizations large and small, with infinite flexibility to choose the components that satisfy real business requirements.

EMM enables IT to easily put its arms around the entirety of data and security concerns in the mobile universe.

How, then, to cross over into a state of enlightenment? What's holding back enterprises from their true potential to wring business value from a mobile strategy can be a lack of systemized thinking about, and integration between, these solutions. This is partly due to a proliferation of vendors, but it is also reflective of the wild card: lines of business and individuals acting outside of IT's supervision. The challenge, then, is for enterprises to develop a posture toward managing mobile that makes sense for their business and will be easy for users to adopt and use, then execute on it effectively.

51 percent of organizations have an enterprise-wide mobility strategy in place with clearly defined initiatives, while 49 percent do not[4]

What's holding back enterprises from their true potential to wring business value from a mobile strategy? It can be a lack of systemized thinking about, and integration between, these solutions.

The final frontier

The universe has now entered an Age of Choice and Plenty, but it is also an Age of Chaos. Today, the people's demands for mobile solutions can significantly outpace IT's ability to satisfy and secure them. Employees want access to business information on-the-go, from their devices.

The lines of business are increasingly realizing the value of allowing access with controls because they see how flexibility can enhance productivity, prevent delays resulting from inability to access corporate systems while on the move, and close security holes that jeopardize precious corporate information. Thus, corporate-owned, personally enabled devices and Bring Your Own Device (BYOD) strategies are rapidly taking hold.

38 percent of companies that push apps to their employees are using customized apps[5]

Typically, most people don't want to carry two devices with different use protocols, data plans, payment schemes, and phone numbers. Some businesses universally allow personal devices to access corporate systems; others block them completely. Some allow applications to be developed and distributed without any thought given to how app and device lifecycles – deploying, updating, securing and decommissioning – will be managed. These approaches are dangerously flawed.

A larger, holistic management system and an associated strategy are both needed to help ensure corporate data security.

Managing an ever expanding universe with ease

Without EMM, IT finds the ever-expanding mobile universe a challenge, and many would be hard pressed to say exactly how many apps are in use and by whom. Apps have fast development cycles, and they can quickly proliferate, given at least three operating systems – iOS, Windows and Android – and dozens of manufacturers of mobile devices.

Making matters worse, cloud-based services have made it easier to download apps, develop new apps, transfer files, and so on – sometimes entirely outside the corporate network.

App development also proliferates because it is decentralized. Say, for example, the marketing department builds a new app in a few weeks and deploys it to staff at a convention, on tablets it purchased, and the app ties into back-end systems. If that happens outside of IT's control or knowledge, that represents a security and management risk. And this type of situation is happening many times a day.

Like the Hubble Telescope, the right EMM solution can provide exceptional visibility into every device entering the corporate datasphere.

IT managers know that mobility is both strategic and inevitable, and want to enable their organizations to stay competitive. On the other hand, IT is faced with responding to a multiplicity of non-standardized platforms and devices, and charged with protecting corporate data.

The questions become:

- How can IT strike a balance between security and productivity?
- How can enterprise IT's mobile agenda integrate with those of multiple vendors?
- How can enterprises that are increasing mobile adoption become both more competitive and more secure?
- How can IT's approach to enterprise mobility move from "IT locks down devices to prevent bad things from happening" to "IT enables previously impossible, good new things to happen"?
- How will the universe become balanced again, yet bathed in light?

Enterprise Mobility Management: At last a comprehensible cosmos

EMM is a solution suite covering the broad spectrum of activities and policies needed to enable mobile user computing across multiple use cases. It's a holistic methodology that can normalize the management of a multi-OS environment, integrate with existing enterprise systems, and securely extend the deluge of data from apps to content.

EMM encompasses all the aspects of mobile management, enabling IT to embrace the ever-expanding mobile universe. It broadens the conversation from a device-centric model to an app- and data-centric model that incorporates enterprise and external applications, data, content, and more in a device-agnostic environment. It subsumes all of the advantages of MDM, MAM, MCM, and containerization into a more flexible structure. EMM can also deliver ROI on mobility, providing executive summaries and deep-dive analytics to help ascertain the true value of mobile connectivity.

EMM empowers businesses to be device-agnostic

EMM releases organizations from having to select one device and operating system to support over others, moving companies away from point solutions that solve only a portion of the larger challenge. It can incorporate both enterprise-developed applications and third-party applications, freeing enterprises to focus on the unique intellectual property embedded in their data. This homogenous approach to managing heterogeneous systems is the panacea of oversight IT has been clamoring for since they took their first MS Cert examination.

40 percent of respondents cited "device choice" as employees' top BYOD priority[6]

EMM is a solution for a global business climate

There's no question that business has increasingly become a global proposition. Where once individual companies went head-to-head, now entire supply chains need to collaborate and compete globally. That means employees and partners are routinely traveling, transacting, and engaging with corporate assets across multiple jurisdictions and cultures.

EMM helps ensure regulatory compliance regardless of location. It allows employees to safely access corporate data on-the-go, regardless of device – including the original mobile device, laptops. It becomes much easier to collaborate, to exchange files, and to synchronize data within and beyond an organization. No matter how people access the network, the appropriate security can be applied.

Popular consumer applications are popular because they're useful. But they weren't necessarily made to interact with systems of record such as ERP and CRM. EMM solutions help bridge these gaps by taking a data-centric approach, generating new potential for return on mobile investment.

EMM: Driving vertical ROI

Even though the number of devices and applications is exploding, it's peanuts compared to the number of businesses and the potential mobile use cases out there. EMM is customizable to the needs of individual businesses, individual departments, employees, and partners. Let's consider a few use cases.

A large industrial company used a network of external agents and contractors to sell products. The company wanted to enable this third-party sales force with applications to help them sell more effectively – but it was not practical for the company to manage their devices, too. The object was simply to deliver apps to the sales force's personal devices and secure the data within the app. EMM helped them assemble just the aspects of mobility management that were needed (MAM but not MDM), providing ease of administration for the company yet non-intrusiveness for the third-party sales force who own their own devices.

A large entertainment company has been able to enhance the customer experience by reducing food and beverage delivery times from an average of 20 minutes to four minutes. Through a specialized mobile app securely managed on tablets used by their staff, customer orders are being fulfilled faster and they are seeing increased revenue from higher order volumes.

Assessing mobility's ROI

A fire department empowered its firefighting crews with iPads that contained floor plans of the buildings in its jurisdiction, as well as live feeds from webcams installed on the properties. In the few minutes between leaving the firehouse and arriving at the fire, emergency responders studied the progress of the fire and gained a better understanding of the building's layout. Being able to get a fire under control 10 minutes faster because it was better understood before anyone set foot on the site returns perhaps the greatest ROI of all: saved lives.

An under-sung aspect of EMM is its analytical capabilities, which can be used to assess the ROI of a particular investment in mobile. For example, insurance companies have historically generated a huge amount of paper. One major US insurer enabled employees to access email from mobile devices and gained the ability to track the times of day email was being sent, and from which devices. The company noticed a significant uptick in after-hours usage on mobile devices – and a corresponding drop in the amount of paper being used, as employees no longer printed work to take home each night. This allowed them to show a clear ROI for their mobile initiative.

Other companies use EMM to analyze the performance and usage characteristics of a particular application or content, giving IT and the line of business managers much better insight into whether it's worth maintaining that investment.

Conclusion

Nearly every enterprise has to deal with mobile devices at a level that was unheard of even two years ago. The array of choices of device, operating system, applications, and potential uses can be dizzying in their infinite scope.

Whether the enterprise needs the entire stack of device, content- and app-management capabilities, and containerization, or just a few, some kind of enterprise mobile strategy is needed. Companies that have deployed EMM have been able to overcome many of the challenges of today's environment, satisfy employee access demands, protect corporate data, and delight management with new potential for productivity and ROI that comes from a mobile strategy. Of course, like any other tool, EMM is not a "magic potion" that operates autonomously. EMM must be guided by a management team thinking about the entire mobile adoption lifecycle that has an appreciation of the challenges and opportunities mobile presents to a company's own specific operating conditions.

We recommend a unified mobile policy for your organization that is much more than an automatic reaction to every new "expansion" from the mobile universe. IT plays a critical role to set different permissions and controls for different groups, and manage these controls through a common system.

Then, the mobile universe will be no less powerful, but may finally be comprehensible, manageable and rational. With this enlightened rationality applied to mobility, you may no longer turn away from the Light, but rocket straight forward, with confidence in the knowledge that its power can be harnessed for good.

This paper was created by CITO Research and sponsored by Fiberlink.

CITO Research

CITO Research is a source of news, analysis, research and knowledge for CIOs, CTOs and other IT and business professionals. CITO Research engages in a dialogue with its audience to capture technology trends that are harvested, analyzed and communicated in a sophisticated way to help practitioners solve difficult business problems.

Visit us at http://www.citoresearch.com

About IBM MaaS360

IBM MaaS360 is the enterprise mobility management platform to enable productivity and data protection for the way people work. Thousands of organizations trust MaaS360 as the foundation for their mobility initiatives. MaaS360 delivers comprehensive management with strong security controls across users, devices, apps and content to support any mobile deployment. For more information on IBM MaaS360, and to start a no cost 30-day trial, visit www.ibm.com/maas360

About IBM Security

IBM's security platform provides the security intelligence to help organizations holistically protect their people, data, applications and infrastructure. IBM offers solutions for identity and access management, security information and event management, database security, application development, risk management, endpoint management, next-generation intrusion protection and more. IBM operates one of the world's broadest security research and development, and delivery organizations. For more information, please visit www.ibm.com/security

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
March 2016

Please Recycle

WGW03109-USEN-01

1 Gartner; http://blogs.gartner.com/eric_goodness/2014/07/30/magic-quadrant-for-managed-mobility-services/

2 Ponemon Institute® Research Report; *2014 "State of Endpoint Risk"*; sponsored by Lumension®; indepentely conducted by Ponemon Institute LLD; publication date: December, 2013;" https://www.lumension.com/Lumension/media/graphics/Resources/2014-state-of -the-endpoint/2014-State-of-the-Endpoint-Whitepaper-Lumension.pdf

3 Donavan, Fred; "*Wanted: Mobile tech strategy*"; surveyed by Robert Half Technology; FierceMobileIT; 3/26/14; http://www.fiercemobileit.com/story/wanted-mobile-tech-strategy/2014-03-26

4 Bernhart Walker, Molly; *"Only half of enterprises have a mobile strategy, security the biggest challenge, says report"*; commissioned by Cisco/Illuminas Survey; FierceMobileIT, 4/1/14; http://www.fiercemobileit.com/story/only-half-enterprises-have-mobile-strategy-security-biggest-challenge-says/2014-04-01

5 Data point taken from Fiberlink's, *"MaaS360 Mobile Metrics,"* May 2014 (no longer posted).

6 Cisco Study: *"IT Saying Yes to BYOD;"* Press release; the network; Cisco's Technology News Site; 5/16/12; http://newsroom.cisco.com/release/854754/Cisco-Study-IT-Saying-Yes-To-BYODwww.maas360.com/maasters/blog security-information/is-your-device-security-policy-leaving-your-company-vulnerable