xtravirt

Mobile Device Management 20 years on

Introduction

In the mid to late 90's, the world of mobility consisted of PDA (Personal Digital Assistant) devices, like the Palm pilot, Psion3, Compaq IPAQ and the Nokia 9000 communicator,

These devices all needed a manual setup to allow them to be able to access email and sync up the calendar and contact information, this was often done using a direct serial cable to sync up with the user's PC.

So, in many large enterprises, administration was a nightmare for IT support teams, having to manually type in the SMTP servers, the user's login credentials and any special setups, like installing certificates, or TCP/IP ports to be directed to. All of this was needed to allow the devices to pick up the user's data, so they could access this information while on the move. The biggest issue was, if the PDA was lost then valuable corporate information could also be lost, as there was no way to remotely wipe the device, or even aid in locating the device.

Rolling out a huge number of these devices to enterprises users, often meant a heavily intensive project and hence was never carried out, except for a select few.

Then in 1999, Canadian company RIM (Research in Motion) launched a unique mobile device called the BlackBerry. This device had the ability to wirelessly link to an organisation's Microsoft Exchange email server, thus enabling users emails to be pushed out to the BlackBerry device, along with their calendar and contacts.

Blackberry 5790

All this was handled by the BlackBerry Enterprise server (BES), which was the first server developed to purely manage the BlackBerry mobile device, and to perform the action of pushing out email and carrying out PIM sync from corporate back office servers. This also meant that these devices could be rolled out in a much easier way than before.

In fact, this was the first enterprise system to be able to control devices on the move. Fast forward 17+ years later to the present day, the BlackBerry is no longer the device of choice and no longer being produced. However, other devices have been developed and taken the BlackBerry's place. The Apple iPhone, launched in the summer of 2008, was the real BlackBerry killer, but by then the mobile market exploded as the Smartphone became of age. Various device manufacturers developed API suites to be able to remotely control their devices, which were then incorporated by various device management software companies. These companies stated their ability to carry out management of these PDA devices, along with so many new functions such as EMM, MCM, UEM, MEM and MDM.

EMM – Enterprise mobile management

UEM – Unified endpoint management

MDM – Mobile device management

MCM – Mobile content management

MEM – Mobile email Management

EMM, UEM and MDM are basically the same description for management of the device, however nowadays devices in addition to the iPhone can be managed and have been expanded to support Apple MacBook as well as Windows 10 laptops.

With the advent of faster cellular technologies, from the earlier GPRS (33kps), 3G (1Mbps) right up to 4G today, and speeds in London reaching 80Mbs, the ability to be mobile, yet still have instant access to all the data held within the corporate network, gives management real worries for the lack of control, loss of data and a real need for monitoring and improved security,

Hence the various device management companies that have come to the rescue, with their own version of MDM.

What is MDM?

Mobile Device Management (MDM) software secures, monitors, manages and supports mobile devices deployed across mobile operators, service providers and enterprises. MDM functionality typically includes over-the-air distribution of applications, data and configuration settings for all types of mobile devices. This includes mobile phones, smartphones, tablet computers, ruggedized mobile computers, mobile printers, mobile POS devices, etc. This applies to both company-owned (COPE) and employee-owned (BYOD) devices across the enterprise or mobile devices owned by consumers.

By controlling and protecting the data and configuration settings for all mobile devices in the network, MDM can reduce support costs and limit business risks. The intent of MDM is to optimise the functionality and security of a mobile communications network, while minimising cost and downtime.

At last this gave the enterprises the ability to remotely wipe a device, perform configuration changes and compliance checks, as well as the ability to distribute updated mobile applications over-the-air and across different device types; the capabilities are endless.

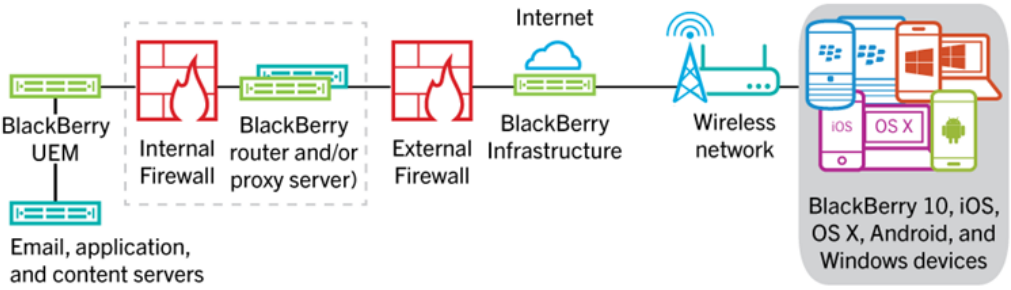
Nowadays, with the addition of GPS being added to the device, it also gives enterprises the ability to locate the device easily.

Every year Gartner, creates a technical comparison paper called, "The Magic Quadrant for Enterprise Mobility Management Suites". In 2012, the choice for an MDM was huge and Gartner had comparisons for 20 MDM companies. Since then, a few have merged and in 2017, they compared 14 different company's products. Of the 14, only 4 have been declared as true leaders; BlackBerry, IBM, MobileIron and VMware AirWatch®, with the leader being the VMware AirWatch product.

AirWatch was founded in 2003, built on the 3 foundation principles of security, multi-tenancy and scalability. In 2014, they were taken over by VMware® and was recently fully integrated into the VMware product suite and renamed as VMware AirWatch. It can be used by SME's, right up to large multi-national companies, like Delta Airways and GSK.

Of the many MDM or EMM suites available, there are only 2 that stand out from the rest. The first, BlackBerry, differs from the rest as all cellular communication occurs via their BlackBerry infrastructure (originally known as network operations centre, or NOC). All enterprise data from a device managed by the BlackBerry agent installed on the device is compressed and encrypted, with AES256 between the Device and the BlackBerry UEM (Unified Enterprise Manager), which is the new name for the BlackBerry Enterprise server.

BlackBerry traffic flow via the BlackBerry Infrastructure



The other MDM that is different to the rest is VMware AirWatch. Three years after the buy-out by VMware, AirWatch has now been integrated into the VMware family, in particular with VMware Identity Manager™ for SSO and VMware NSX®. AirWatch also provides the power behind the VMware Workspace™ ONE™ product, thus providing the complete end-user computing needs for any company requiring a fully integrated management of corporate devices. AirWatch comes as a SaaS, dedicated SaaS and on-premise offering. This too has the capability for end to end encryption, with VPN's.

The other big differentiator with AirWatch is its multi-tenant capabilities. Below is a diagram showing a sample of the AirWatch multi-tenancy capabilities, the image on the right is an extract from the AirWatch Admin console

Multi-tenancy map of the World-Wide Enterprise

Looking through the structure, very quickly you can see that it is similar to a multi-national company, in this case "World Wide Enterprise" (WWE) which is the top level globally, and from there you drill down to regions, countries, and then divisions. At any of these levels, you can define application profiles, compliance policies, privacy setups, terms of use, as well as different email and Active Directory servers - plus it gives the IT teams the capability to handle personal and corporate devices with ease.

With the WWE example, you can define a different AD for the Middle East from the UK, use a IBM domino server for email in the UK, while USA uses MS Exchange and have different privacy policies for Germany from the rest of the organisation. This enables you to comply with different laws and legislations of each of the individual countries your organisation covers.

Therefore, you can also have a different set of apps assigned to the UK, over say, France, because of a requirement for localised application.

It's worth noting that these controls are hierarchical and the settings will percolate down through the chain by inheritance, however the security can be increased at any point down the chain. This means that if at the Global WWE level, a passcode is set to be 4 characters long, but the UK requires 6 digits, then this can be changed (by overriding) and this will then be cascaded down to all the divisional offices in the UK region. With this capability, you can easily define a global security requirement for all your different divisions.

AirWatch also has the capability to sync up user groups defined in the corporate directory services (Active Directory / LDAP) and can automatically add those users into AirWatch, consequently creating a user profile. It can then easily be ensured that the user groups are sync'd twice a day and if a user is removed, then the user will not be able to re-enrol.

Users are first created in the AirWatch region that they are going to operate in (e.g. World Wide Enterprises/NA/Corporate/Sales) and then are assigned with the "Smart Group" created for that region and role.

Smart Groups are customisable groups, that are assigned to a particular organisational unit, and will automatically assign the attributes (Device profiles, Applications, compliance policies, VPN and Wi-Fi) that had been applied to the smart group. Smart Groups provide you with the flexibility to deliver content and settings by device platform, model, operating system, device tag or user group. You can even deliver content to individual users across multiple organisation groups and regions, as the smart groups have the ability to transcend the whole of the corporate organisation tree within AirWatch.

Users can also be simply moved within the AirWatch Admin console to another region with ease. AirWatch manages the change automatically and the old smart group can automatically be removed and the new one assigned to the new location put in its place.

So, the Multi-tenancy and Organisation group capability along with Smart Groups sets AirWatch apart from the rest of the MDM/EMM suppliers, ensuring that the administration of all the users and devices is carried out with ease and in a secure fashion, with all of this communication encrypted.

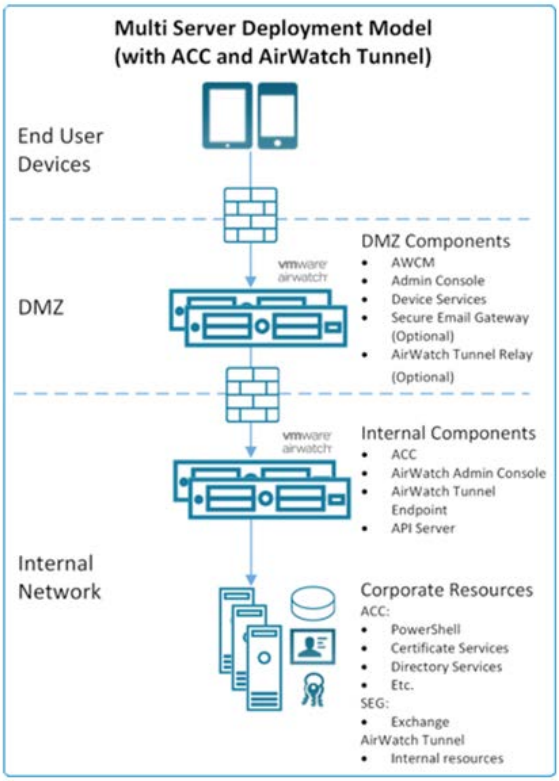
Design

Often the MDM system can be observed as a single black box, the design of the end solution is determined by what it will be used for, for example, a small company with 20 users, needing a standard mobile control (like remote wipe of device if lost and ability to remotely change the password) and to receive email, will be different to a large international company with a global estate of 100,000 devices to manage, and requiring a fully secured access into the corporate environment, including SharePoint.

But the rollout of an MDM can save the enterprise money. As a perfect example, Delta airline decided to replace all of the heavy 45 lb pilot's cases, which held flight plans, charts, reference documents and other information for the pilots during their flight, with an electronic flight bag (Apple iPad) managed by AirWatch, for its 11,000 pilots. Delta estimates that it can save $13 million in fuel costs by replacing the paper manuals.

Some companies have to ensure that all data is held in a secure UK based unit, especially government departments, so they have the AirWatch MDM on premise system installed. There is often a requirement for High Availability, hence the on-premises systems are setup in 2 different locations to provide this, using AirWatch MDM running VMware vSphere, vMotion and HA.

On-Premise deployment of AirWatch EMM



Security

With the persistent threats of Malware and other security breaches on mobile device, solutions are required to be put into place to ensure that enterprise data is held on the device in a secure environment.

Both Apple and Samsung have ensured that by default, the data on the device is fully encrypted and that device enrolment is simplified. Both have enrolment platforms in place that ensure that after a device wipe, and upon gaining access to the internet (by Wi-Fi or by a mobile carrier's portal), they check to see if the device is part of an enrolment platform. This is done by checking the device serial number. If is found to be listed, then the enrolment platform will go to the corporate MDM solution that the device is enrolled into, and the assigned MDM profile is picked up and forwarded to the device. By enrolling a device into the associated program, the MDM profile cannot be removed, except by the MDM admin team - even a reset to factory won't stop this occurring.

Both Samsung and Apple also increase the number of IT policies to control the device when part of these enrolment programs, and are managed alongside the MDM. AirWatch supports both of these enrolment programs.

AirWatch MDM also has the ability to check if the device has been rooted or "jailbroken". This is when a modified operating system is installed on the device to give the user a higher level of access to the device, however in doing so, it can also be more prone to malware. If an AirWatch compliance system decides that a device is rooted, it is highlighted to the admin team. AirWatch policies can however force a number of processes to be carried out, including removing all enterprise data from the device.

AirWatch works closely with mobile device manufacturers to ensure that on the day a new OS update for a device is released, AirWatch is able to support it.

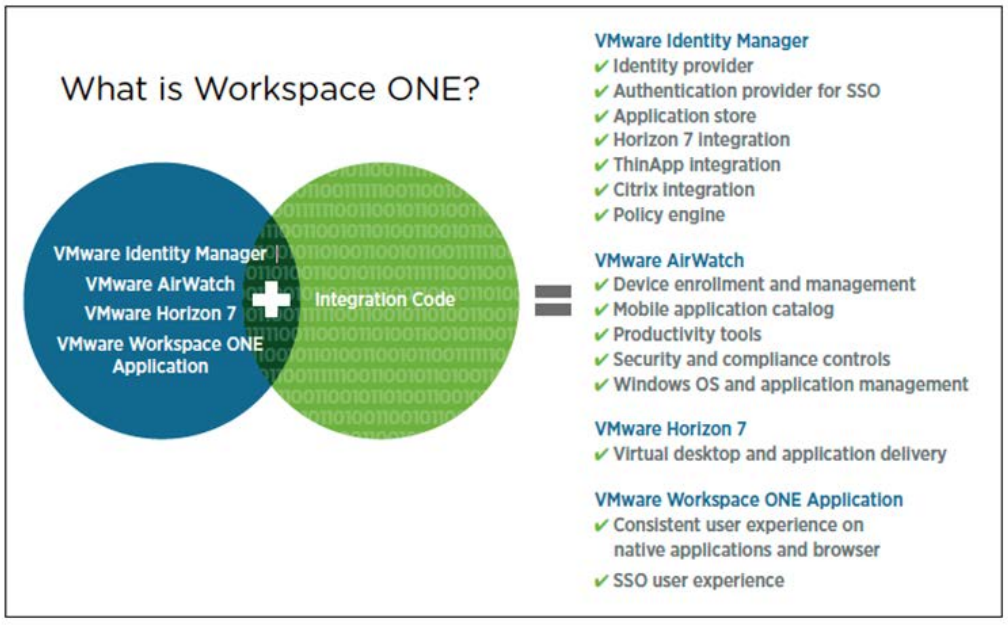
IT support is also made easier, by the ability for administrators to be defined by roles within the admin console, from AirWatch Administrator to Help Desk, with the resulting admin console menu reflecting only what has been set for that particular role. There is also a custom role capability if the existing roles need to customised, so the normal password reset type calls can be done by less experienced staff who would have a restricted menu of tasks that they can perform.

Single Sign on & integration with Office 365

VMware has in its recent release of AirWatch, combined the VMware AirWatch EMM with the VMware Identity Manager and VMware Horizon 7, enabling a true mobility offering that brings aspects of each package together into one.

This enables the user to only need a one-touch sign in and be authenticated to install and use the application in the App store, without the need to keep authenticating. You can deploy the Office 365 apps onto the managed devices and then use them with ease. It does this by using SAML, the open standard for SSO across multiple services, it also interoperates with other identity providers, like Microsoft Azure.

Capabilities of Workspace ONE



The role of an MDM consultant

The role of an MDM consultant, requires not only the experience of designing and administering the MDM solution, but also an understanding of the end user devices, the networks, security and system requirements that an MDM solution will be required to work with. They will also require an understanding of how various mobile applications interact with the mobile architecture.

Issues selecting the right device can also have a huge impact on the control of the devices. There are numerous android based devices available these days, however care is needed in selecting the devices, as the cheaper one may only support the basic options that Android includes in its core OS.

The easiest way to assess these devices is to look at the MDM device profile screen and see which device supports the required IT policy. Not all are the same, especially in view of the various regulatory bodies that impose rules on mobile devices. If a government department needs devices set to an "official" level of security classification, then the device that would need to be selected is the Samsung Galaxy S7 device or above, which is capable of using the Secure Knox container, all of which is controllable by AirWatch.

Typically, during an AirWatch project, a consultant is called in after the company has decided to start a Proof of Concept MDM project with their IT team. More often than not, this rapidly turns into a live environment, without any thought put in to the planning for how it will be most effective for the organisation. This causes a lot of extra work in rectifying the POC setup along with delays, especially if they then need to ensure that the "live" users are not affected in any way by the changes.

If an enterprise was looking to implement an MDM solution, it would save a lot of time and effort if an experienced MDM consultant was to be place within the project team and involved with the actual MDM implementation. Then, from the outset, a managed flow of meetings and investigations can be carried out to get the actual live requirements from the stakeholders, users, departments and management; all of which are combined into a high-level design document, that gets senior management approval, prior to starting the project. This makes the whole implementation process much easier and with VMware virtualisation products, the technical requirements can be easily managed and adjusted, according to the computing needs obtained during the performance monitoring process.

MDM solutions are highly configurable, and powerful, but by using an experienced Mobility consultant, the ROI will be seen much quicker and become a more effective solution than carrying out a POC blind.

The future of device management

With the rapid expansion of IOT and devices like Google Glasses (which is now being used within manufacturing) device management is moving into new areas, especially in industry and around the security aspect.

MDM providers can already manage data capture devices and printers, for example from the Zebra Technologies range.

Tablets are now found in restaurant and retail sites, configured for single app use and used as the interface into local stock control or ordering food in a restaurant & paying the bill, rather than going to a cashier desk.

The education market is also seeing a major boost. Ensuring devices are secure is now more important than ever, to prevent children by-passing the security barriers put in place.

All of these new applications mean that MDM is a growing and vital area for all types of organisations to be considering, and should play a key part of any IT strategy.

Xtravirt understand how to help organisations get the most from their workspace environment. We can work with you to advise, design, build and deploy the right solution for your organisation to help you plan for success and better serve your customers. To find out how we can help, contact us and we'd be happy to use our wealth of knowledge and experience to assist you.

About Xtravirt

Xtravirt are an experienced consulting firm dedicated to delivering outcomes to help customers solve their IT challenges. We design and build strategies to help customers unlock the full potential of cloud, datacentre and workspace technology.

We are the VMware Global and EMEA Professional Services partner of the year 2017/18.

www.xtravirt.com

Email info@xtravirt.com **Tel** +44 (0)800 4880 038 **Web** xtravirt.com