Enterprise Mobility Management Smackdown

Author(s) : Peter Sterk, Ruben Spruijt

Version: 1.1

Date: June 2013

Eenvoud in ICT

© 2013 PQR, all rights reserved.

All rights reserved. Specifications are subject to change without notice. PQR, the PQR logo and its tagline Eenvoud in ICT are trademarks or registered trademarks of PQR in the Netherlands and/or other countries. All other brands or products mentioned in this document are trademarks or registered trademarks of their respective holders and should be treated as such.

TABLE OF CONTENT

1. Introduction 4

1.1 Objectives 4
1.2 Intended audience 4
1.3 Vendor Involvement 4
1.4 Suggestions and Improvements 4
1.5 Contact 5

2. About 6

2.1 About PQR 6
2.2 Acknowledgments 6

3. The Bento Box of Mobile IT 8

3.1 The Bento Box Bliss of Enterprise Mobility 8
3.2 Consumerization of IT 8
3.3 Application delivery: 3-2-1 and action! 9
3.4 Mobile Application Delivery 11
3.5 IT as a Service and tomorrows IT organization 12
3.6 Bento?! 13
3.7 Enterprise Mobility Management 2013 by Jack Madden 13

4. Application and Desktop Delivery Solutions 3.0 14

4.1 ADD solutions overview 3.0 14
4.2 Trusted and untrusted work place scenarios 14
4.3 Secure access 15
4.4 Mobile Application Delivery 15
4.5 Web application acceleration 15
4.6 Connection broker 16
4.7 Application virtualization 16
4.8 OS provisioning 17
4.9 Server-Hosted Desktop Virtualization (VDI) 17
4.10 VDI with GPU acceleration 17
4.11 Session Virtualization (TS) 18
4.12 Client-Side virtualization 18
4.13 Workspace Aggregation 18
4.14 Client management 19
4.15 Vendor matrix, who delivers what 20

5. Security 22

5.1 Main Challenges 22
5.2 The Goal 23

5.3 Vision....24
6. Mobile IT Strategy....25
7. Enterprise Mobility Management....28
7.1 Introduction....28
7.2 Mobile Device Management....28
7.3 Mobile Application Management....29
7.4 Mobile Information Management....30
7.5 Mobile Expense Management....31
7.6 Secure e-mail....31
7.7 Secure Data, Enterprise FileSync....32
7.8 Secure Web browsers....32
8. Vendors and their EMM Solutions....33
8.1 Introduction....33
8.2 AirWatch Enterprise Mobility Management Suite....33
8.3 AppSense EMM Suite....36
8.4 Cisco Meraki Systems Manager....40
8.5 Citrix XenMobile....41
8.6 Good for Enterprise....44
8.7 MaaS360 by Fiberlink....49
8.8 Microsoft Exchange ActiveSync....53
8.9 Microsoft Windows Intune....53
8.10 MobileIron....56
8.11 Symantec Mobile Management Suite....59
8.12 VMware Horizon....64
9. EMM features Comparison....70
9.1 Introduction....70
9.2 Compare Matrix, Quick reference....71
9.3 Roadmap and Future additions....71
9.4 Product Version....72
9.5 Feature Compare Matrix....72
9.6 Compare Matrix, Features....73
10. Change Log....86
11. Appendix: A-Team (PQR) members....87

1. INTRODUCTION

Do you want to know the real difference between “Mobile Device Management” and “Mobile Application Management”? Do you want to know the role of Enterprise Mobility in BYO and Consumerization of IT? Are you looking for insights into Enterprise Mobility in Application and Desktop Delivery? Are you looking for an independent overview of the Enterprise Mobility Management (EMM) solutions and curious about the different features- and functions each EMM vendor is offering? If so, this is the whitepaper you MUST read!

In the current market, there is an increasing demand for unbiased information about Enterprise Mobility Management (EMM) solutions. This white paper focuses on solutions that are anticipated to have an important role in Enterprise Mobility Management. An overview of features has been created to enable a better understanding and comparison of capabilities.

1.1 OBJECTIVES

The goals of this whitepaper are to share information about:

- Application and Desktop Delivery in the mobile world
- Consumerization, BYO in tomorrow’s workspace
- Enterprise Mobility Management Solutions
- Explain the different Mobile Managements concepts
- Explain the pros and cons of the different Mobile Managements concepts
- Describe the different Enterprise Mobility Management (EMM) vendors and solutions
- Compare the features of the various EMM solutions

1.2 INTENDED AUDIENCE

This document is intended for IT Managers, Architects, Analysts, System Administrators and IT-Pros who are responsible for and/or interested in designing, implementing and maintaining Enterprise Mobility Management solutions.

1.3 VENDOR INVOLVEMENT

All major vendors whose products are analyzed and described in the feature comparison have been approached in advance to create awareness of this whitepaper and discuss the different features and functionality.

1.4 SUGGESTIONS AND IMPROVEMENTS

We’ve done our best to be truthful, clear, complete and accurate in investigating and writing down the different solutions. Our goal is to write an unbiased objective document where possible, which is valuable for the readers. If you have any comments, corrections or suggestions for improvements of this document, we want to hear from you. We appreciate your feedback.

Please send e-mail to Peter Sterk (pst@pqr.nl) or Ruben Spruijt (rsp@pqr.nl) include the product name and version number and the title of the document in your message.

1.5 CONTACT

PQR; Tel: +31 (0)30 6629729

E-mail: info@pqr.nl ; *www.pqr.com;* Twitter: http://www.twitter.com/pqrnl

THIS DOCUMENT IS PROVIDED "AS IS"
WITHOUT WARRANTY OF ANY KIND
FOR REFERENCE PURPOSES ONLY

COPYRIGHT PQR

IT IS NOT ALLOWED TO (PARTIALLY) PUBLISH OR DISTRIBUTE CONTENT WITHOUT APPROVAL

2. ABOUT

2.1 ABOUT PQR

PQR is a professional ICT infrastructure company focusing on the availability of data, applications and workspaces with optimized user experience in a secure and manageable way. PQR provides its customers innovative ICT solutions, from on-premise to cloud management, without processes getting complex. Simplicity in ICT, that's what PQR stands for.

PQR has traceable references and a wide range of expertise in the field, proven by many of our high partner statuses and certifications. PQR is a Citrix Platinum Solution Advisor, HDS Tier 1 Platinum Partner, HP GOLD Preferred Partner, Microsoft Gold Partner, NetApp Star Partner, RES Platinum Reseller, VMware Premier Partner en VMware Gold Authorized Consultant Partner. PQR's approach is based on four main pillars:

- Data & System Availability
- Application & Desktop Delivery
- Secure Access & Secure Networking
- Advanced IT Infrastructure & (Cloud) Management

PQR, founded in 1990, is headquartered in De Meern and has over 107 employees. In fiscal year 2011/2012 posted sales of € 94.9 million and a net after tax profit of € 4.6 million have been recorded. www.pqr.com

2.2 ACKNOWLEDGMENTS

Team leaders:

Peter Sterk is a solution architect at PQR. In this position, he supports customers with any technical challenge they may encounter, following PQR's credo 'Simplicity in ICT'. Although he is focused on Enterprise Mobility, Application, and Desktop Delivery, Peter is also able to overlook and advise on other components in IT infrastructures. Peter is active in communicating the vision of PQR on subjects like Application and Desktop Delivery and Enterprise Mobility on various national and international events. You can contact Peter at pst@pqr.nl or on twitter

Ruben Spruijt is CTO and focuses primarily on Enterprise Mobility, Virtualization, Application and Desktop Delivery – tomorrow's workspace. He is actively involved in determining PQR's vision and strategy. Ruben is a Microsoft Most Valuable Professional (MVP), Citrix Technology Professional (CTP) and VMware vExpert and is the only European with these three virtualization awards. He gives customers advice and has them benefit from his expertise; he motivates his colleagues and writes blogs, articles and opinion pieces on a regular basis. During presentations in several national and international congresses, Ruben shares his thoughts and knowledge on application and desktop delivery, and on virtualization solutions. To contact Ruben at rsp@pqr.nl or on twitter

A-Team!

Only through the effort and persistence of the 'EMM Smackdown' team, we achieved the goals, a big thanks to them!

Name	Position	Contact	Role	Twitter
Henk Hoogendoorn	Consultant PQR	hho@pqr.nl	Writer	@henkhoogendoorn
Marcel van Klaveren	Consultant PQR	mkv@pqr.nl	Writer	@itguru3
Anton van Pelt	Consultant PQR	ape@pqr.nl	Writer	@antonvanpelt
Sven Huisman	Consultant PQR	shu@pqr.nl	Writer	@svenh
Erik van Veenendaal	Consultant PQR	eve@pqr.nl	Reviewer	@evveenendaal
Cor Reinhard	Consultant PQR	cri@pqr.nl	Reviewer	@correinhard

Thanks for reviewing and feedback: Bob de Kousemaeker, Gerjon Kunst,

Special thanks to Alistair Gillespie

A special thanks to **Alistair Gillespie** for reviewing the document and provide great feedback. He is based in the UK and works in the End User Computing space covering Client Virtualization, Application Virtualization and Enterprise Mobility. To contact Alistair directly email or follow Alistair on twitter.

Special thanks to Erik Remmelzwaal and DearBytes

Erik Remmelzwaal In 2001, while studying Commercial Economics in Haarlem, he became an intern at the start-up company, Medusoft (later DearBytes). Erik continued to work for Medusoft following his internship, focusing on customer technical support; first as Consultant and later as Team Leader. After the company was taken over in 2010, Erik was appointed CEO. The company, which now serves more than 1,000 organisations, changed its name to DearBytes in 2012. This better reflects the organisation's new positioning and activities.
At work Eric still gets most enjoyment from talking to customers about the challenges they face controlling their information security. He enjoys being available for such sessions, and can be reached easily via LinkedIn and Twitter.

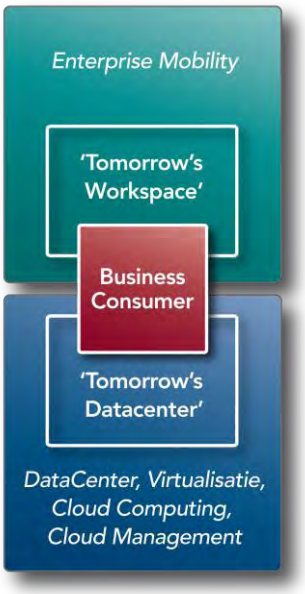
DearBytes helps organizations gain and maintain control over the security of critical assets and information. As a security service provider, DearBytes has extraordinary insights into the daily; real world challenges companies' face controlling security. The solution-driven attitude of DearBytes led to the development of various tailor-made solutions such as Dear360 (security risk management), Bytescan (second opinion), and its highly valued managed services program.

3. THE BENTO BOX OF MOBILE IT

3.1 THE BENTO BOX BLISS OF ENTERPRISE MOBILITY

Enterprise Mobility, Big Data (and analytics), Social Collaboration, Cloud computing and management are the top priorities of IT Executives in 2013 and 2014.

Empowering the end-user by giving access to Windows, Web and Mobile applications so they can access data and information systems from both private and public datacenters regardless of the device or location is the ultimate strategic objective for 'tomorrow's workspace'. While tomorrow's workspace is direct attached to the end-user, the business consumer, it's important to understand the role of 'tomorrows datacenter' and 'tomorrows IT organization' to use the full potential.



What are the key components in tomorrow's workspace?

- It is all about '**Me'**: User, Business Consumers.
- **Any**x7 (Device, Screen, Location, OS, Application, Browser) Online/Offline, Managed/Un-Managed**.**
- **Access**: Data, Apps, Identity, Aggregated, Networking.
- **Apps**: Apps, Applications, Web/SaaS, Mobile.
- **Devices**; three screens + Hybrids.
- **Managed**; None/nothing, Device, Apps, Data.
- **SelfService**; IT Store.
- **Context** Aware: personalized.
- **Collaboration**; Social, Unified Communications, Mesh.

3.2 CONSUMERIZATION OF IT

"Consumerization of IT is the growing tendency for new Information Technology to emerge first in the consumer market and then spread into business and government organizations. The emergence of consumer markets as the primary driver of information technology innovation is seen as a major IT industry shift, as large business and government organizations dominated the early decades of computer usage and development" (source)

Today's challenge is that users expect to be able to work from any location, on any device, accessing all of their apps … while IT maintains compliance, protects data and reduces risk and costs.

One of the most important trends in IT is "Consumerization of IT". Consumers are used to great usability, app stores, tablets and smartphones and business consumers expecting no less from their own IT. Users with little or less IT background are able to select, download and install applications without the blink of an eye.

In our industry, organizations and IT professionals need to create a mind shift to solving these challenges. The following topics are part of this mind shift and the broader discussion:

- Consumerization of IT is here to stay; the Business Consumer controls 'IT' / 'it'.

- Bring Your Own Device (BYOD) is the new normal, but BYOD is not for everyone or in every situation.
- Self-reliant, self-supporting, freedom and control needs to be in balance. This balance will vary based on the context such as user role, location, device, security.
- Managing expectations from Business Consumers to IT.org and from IT.org to the Business consumers is key in the paradigm shift called Consumerization of IT.
- It is AnyAnyAnyAnyAnyAnyAnyAny; AnyDevice, AnyScreen, AnyLocation, AnyOS, Any-Browser, AnyApp, AnyOne; Managed, UnManaged, Online and Offline. Design for change.
- It is not about (managing) the device or application but about data.

The three letters BYO an acronym for one of the hottest trends. 'Bring Your Own', 'Buy-Your Own' … in the grand scheme of solutions it's more about 'Who owns the device', what is the balance between self-reliant, freedom and control. Do you need control? If you need control.. Control on what… Device/Application/Data?

Key components in the Bring Your Own (BYO) strategy are:

- Enterprise App Store;
- Enterprise Mobility Management (EMM);
- Secure Access, Secure Networking;
- FileSharing;
- Unified Communications, collaboration and Social Media for the Enterprise;
- Rich Mobile and Web Application delivery options;
- Windows Desktop and Application Delivery options.

3.3 APPLICATION DELIVERY: 3-2-1 AND ACTION!

Application Delivery is a crucial part of a user's workspace, the goal is to make applications available independent of location and device, so users can work onsite, online, offsite, offline, anywhere, with any (own) device and at any time. The dynamic delivery of applications is an essential functionality and part of a broader workspace strategy. It's important to understand the various application and desktop delivery concepts - "the bento box". To enable this PQR have created an at-a-glance schema of the various application and desktop delivery solutions. A detailed view of the just released solution schema can be found in chapter 4.

When investigating which application delivery solutions will work best for your organization, it is essential to ask three questions:

1. What is the **execution** platform for the **applications**? Within the execution platform, system resources are used in order to execute the windows, web-architected, rich

mobile and mobile web-applications. The most frequently used execution platforms include the following: Desktop, Laptop, Ultrabook, Tablet, Smartphone, Virtual Desktop Infrastructure and Server Based Computing (also known as Session Virtualization). The choice of an execution platform is the most fundamental decision made! Applications are executed either locally on a device or centrally in a datacenter. Each execution platform has its own characteristics. In practice, every organization possesses a mixture of device access scenarios. The theories: “Less is more”, “Cut out the exceptions” and “Manage diversity” should always be in mind!

2. How will **applications** be made **available** on the execution platform? An execution platform is great; but if there are no applications available on the platform, the platform is of no real value to the end-user. The second question is this: How will applications get onto the execution platform?! A number of solutions exist for making Windows, web-architected, rich internet and mobile web applications available on the platform.

3. How are the execution platform and the applications **managed** from an IT-Pro and from an end-user perspective? An execution platform with a variety of windows, web and mobile applications can be created but how do you manage and maintain this environment?

Important points to keep in mind:

- What are the different access scenarios, personas?
- In a Bring Your Own Device (BYOD) scenario where does managing the environment start and where does it ends.
- Do you need to manage the Devices, Apps, Data?

These and more questions fit in this third question: How do we control, maintain and support the workspace as a concept and as an endpoint device from an IT Pro and end-user perspective?

The ‘Enterprise Mobility Management’, ‘Workspace Aggregation’ and ‘User Environment Management’ solutions fit in this third, management category. With a wide range of concepts, functionality and technology available, it is critical to understand what Enterprise Mobility (EM) will bring for ‘Me’ as a user.

This Enterprise Mobility Management Smackdown whitepaper is intended to help understand the impact and role of Enterprise Mobility Management in ‘Tomorrow’s Workspace’.

3.4 MOBILE APPLICATION DELIVERY

There are various ways to deliver applications to mobile devices such as Apple, Google, Black-Berry, Microsoft smartphones and tablets.

- Deliver Windows Apps and Desktops via Server Hosted Windows solutions.
- HTML5 and (Mobile) Web Apps.
- Rich Mobile Applications.

3.4.1 Deliver Windows Apps and Desktops via Server Hosted Windows solutions

In this scenario, Windows applications are executed in the datacenter and presented locally on the mobile device. The benefit is that execution and presentation of the application is separated, (unmanaged) device independent and 'classic' applications can be used without (re)developing the Business Applications. With this solution, there is less discussion about managing the device and controlling the data flow. The downside is that it only works in a (well) connected networking scenario and more importantly, the Windows applications and desktop are designed for mouse, track pad, keyboard and larger screens. There are solutions in the market known as "app refactoring" tools such as the Citrix XenApp Mobility Pack which can be used to configure Windows application interfaces optimized for mobile devices.

Our starting point in this discussion is *"deliver Windows 'classic' applications or desktops to mobile devices, such as smartphone and tablets, is the best choice when you have run out of other options".* At the end of the day, most Business Consumers want to use (near) native apps that are designed and optimized for mobile devices.

3.4.2 HTML5 and (Mobile) Web Apps

Most of today's corporate web-architected applications are not HTML5 but just traditional web applications. Web-architected applications are OS and browser independent and will work over LAN, WAN, WiFi and internet connections. These applications will work on mobile devices as well, but are not designed and therefor optimized for mobile device platforms. Web-architected applications can solve portions of the mobility problem but one of the main questions is: what is the user experiences and does the solution meets the user's perceived performance?

HTML5 seems to be the ultimate solution, the future of mobile apps delivery. Apps can be used offline, HTML5 apps are platform/ browser independent and apps can have an interface optimized for mobile platform using the device APIs. Despite the advantages of HTML5 apps there are downsides as well. HTML5 apps will be limited by the browser on the mobile platform, not all browsers do support all features such as offline storage or push notifications. Also the level of control over how HTML5 apps can interact with the rest of the mobile platform can be challenging.

3.4.3 Rich Mobile Applications

The majority (~98%) of mobile applications are delivered via the consumer app stores such as Google Play Store, Apple App Store or Windows Store. Mobile Application Management (MAM) solutions cannot manage these applications because the apps are isolated / sandboxed

on the mobile device by design. How do we get mobile (business) applications on our mobile devices so we can manage them? Approaches include:

- MAM vendor supplied SDK
- App wrapping

Use the Software Development Kit (SDK) from the MAM vendor so you can ensure that management features are hooked in the mobile applications from the start. The caveat is that the intelligence offered by the SDK needs to be included while developing and compiling the application. This is fine for an in-house application, which is built and distributed by the organization but will not work in most of the commercial (or free) public applications.

App wrapping is the approach where commercial public applications binaries are wrapped with a management layer that gives the MAM solution the control it needs. The biggest problem with that is Digital Rights Management (DRM) and encryption is built into the mobile platforms, which blocks App wrapping technologies for Mobile applications where you do not get access to the (unsigned) source binaries. When you have access to the source binaries, the App wrapper tool will add Management capabilities such as authentication, (application level) VPN support, Device Policies, Remote Kill switch, encryption etc. The application will be packaged, re-signed and distributed as an in-house developed application through the corporate application store functionality of the MAM solution.

3.5 IT AS A SERVICE AND TOMORROWS IT ORGANIZATION

Business Consumers expect or demand solutions. If the IT organization does not deliver end-user will often go and find solutions elsewhere. ShadowIT or 'StealthIT' is the term used to describe IT solutions used inside organizations without organizational approval. StealthIT solutions are not often in line with the organization's requirements for control, security, reliability, documentation etc. To solve ShadowIT we need to think of 'IT as a Service'.

Key components of IT as a Service are:

- Self-service;
- Reliable and personal;
- Context aware;
- Automated and Secure;
- Pay per Use (charge,- show back);
- Using Private, Public or Hybrid Cloud solutions.

The 'IT organization of tomorrow' should act as providers of their own IT services and intermediary of public cloud services delivering and govern these services to their business consumers.

3.6 BENTO?!

Perhaps you thought - why is Chapter 3 called "The bento box bliss of Enterprise Mobility Management"? Well - a bento is a single-portion takeout or home-packed meal common in Japanese cuisine. A traditional bento box or container holds a variety of delicious food. Japanese homemakers often spend time and energy on a carefully prepared lunch box for their spouse, child or themselves. Enterprise Mobility, or MobileIT is also a bento box. It consists of a variety of solutions so Business Consumers can access data and information systems regardless of the device or location enabled via a range of application delivery solutions.

"In a time of rapid change, standing still is the most dangerous course of action" and "when opportunity comes, it's too late to prepare"

We hope that this whitepaper will be helpful so you are fully prepared for 'tomorrow's workspace'

3.7 ENTERPRISE MOBILITY MANAGEMENT 2013 BY JACK MADDEN

Jack Madden is an independent blogger, co-author of The VDI Delusion book and speaker at events like BriForum and Citrix Synergy. In May 2013 Jack Madden will publish his new book Enterprise Mobility Management 2013. Jack Madden will dig into the rapidly-changing EMM field that has emerged in the post-BlackBerry era—the world of MDM, MAM, MIM, app wrapping, containers, file-syncing, SDKs, mobile virtualization, and BYOD.

"This book is for anyone who's noticed the hype around enterprise mobility management: It's for people who've heard of MDM and want to know how it works. It's for people who have observed the debate between MDM and MAM vendors and want to know how they fit together. It's for people who've heard ominous warnings about the dangers of BYOD and want to see what the big deal is.

And this book is for users who want to understand what their company is doing; users who think it's ridiculous that they have separate work and personal phones. It's for users who don't want to give up control of their phone to their company. And it's for users who just want to be able to bring in a phone or tablet in the first place.

Finally, this book is for companies which have built their mobility plan around BlackBerry Enterprise Server and now must figure out how to move on. It is for desktop people who are now tasked with delivering applications and data to new platforms. It's for the mobile managers who were happy with Blackberry for the past 10 years and now have to deal with users bringing in iPhones."

Be sure to read this book for even more (background) information on the changes that Enterprise Mobility Management brings for users and companies. A must read!

4. APPLICATION AND DESKTOP DELIVERY SOLUTIONS 3.0

4.1 ADD SOLUTIONS OVERVIEW 3.0

Before doing a 'deep dive' into Enterprise Mobility Management, it is important to have an overview of all the 'Application and Desktop Delivery' solutions. PQR created the "**Application & Desktop Delivery Solutions Overview**" to provide an at-a-glance outline of the various application and desktop delivery solutions. Reading this chapter will give you a complete outline of the diagram and all the application and desktop solutions that are included within it. This paragraph does not aim to describe all application scenarios or their technical advantages and disadvantages, but to give a general idea of the state of union in the application and desktop delivery segment, independent of vendors.

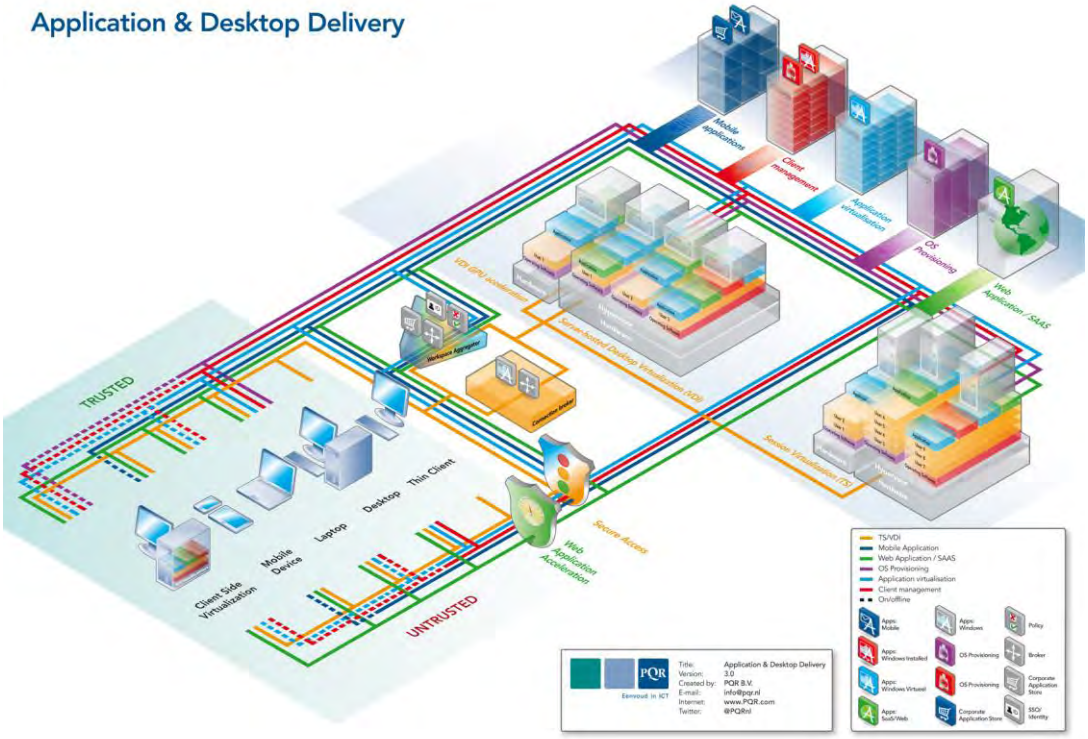


Figure 1, Application and Desktop Delivery Solutions Overview

4.2 TRUSTED AND UNTRUSTED WORK PLACE SCENARIOS

Trusted work places are devices that are connected to the existing IT backend infrastructure via wired or wireless network. Untrusted work places are devices that do not have a secure wired or wireless network connection to the existing IT backend infrastructure or devices which aren't centrally managed by the IT department. This is, for example, equipment that is connected to a separate network segment for security reasons or because it is used from home or at a work experience location.

Each organization has different work place and application delivery scenarios, especially with Bring Your Own Device (BYOD) and Enterprise Mobility the amount of scenario's will increase rapidly. For the IT department, it is important to have a good overview of the various work place and application delivery scenarios, we call this persona or access scenario's, since this indicates how the various users work with the applications and what their requirements are.
In the work place scenario's we see 'Client Side Virtualization', Mobile Devices such as smartphones and tablets, Laptops and (Hybrid) Ultrabooks, Desktops and ThinClients being used.

4.3 SECURE ACCESS

Secure Access solutions provide secure access for (untrusted) devices to corporate IT. A Secure Access solution could be a full (SSL) VPN solution or a Gateway Services which is targeted for Server Hosted Desktops. Solutions that can be used to realize secure access scenarios include Cisco ASA, Citrix Netscaler Gateway, Juniper SSL VPN, Microsoft Unified Access Gateway (UAG) and VMware View Security Server. A complete overview of Secure Access and Secure Networking solutions has been created and can be downloaded from www.pqr.com
Functions of Secure Access are:

- Secure Network access, the shield symbol.
- Access to corporate resources, the traffic light. Access can also be fine-grained.

4.4 MOBILE APPLICATION DELIVERY

Rich Mobile applications running natively on Apple iOS, Google Android, Blackberry, Windows Phone and Modern Apps on RT or Windows 8.x are delivered by the Mobile Application delivery solution. In enterprise customer scenario's this function is incorporated in most of the Enterprise Mobility Management solutions but it can be a more consumer focused application store as well. Functions of mobile application delivery are:

- Store - a user interface for application access, delivery and reporting functionality.
- Delivery of Rich Mobile Application to a variety of mobile devices.

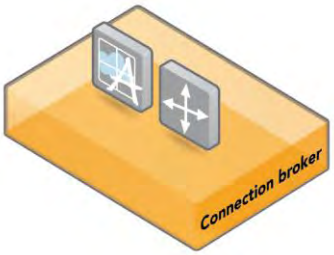
4.5 WEB APPLICATION ACCELERATION

Web Application Acceleration appliances, or application delivery controllers accelerate and secure web-architected applications. We are all confronted with these solutions nowadays: Public facing internet applications such as Google, MSN and eBay all use them. Web Application Acceleration solutions are not just useful for large public organizations, you can also use them for your own web applications. Solutions that facilitate web application acceleration and security include packages such as Citrix Netscaler and F5 BigIP.
Functions of Web Application acceleration are:

- Secure access to SaaS and Web resources, the shield symbol.
- Fast and optimized access to web applications, the accelerator symbol.

4.6 CONNECTION BROKER

A connection broker determines which server-hosted remote applications and desktop will be available to a user. When using a server-hosted virtual desktop infrastructure, it's possible to either designate dedicated desktops or a pool of remote desktops.
The desktop broker can automatically create, remove or pause remote desktops. There are a number of connection broker suppliers. Citrix - "XenDesktop", Microsoft - "Remote Desktop Services", Dell/Quest - "vWorkspace" and VMware - "Horizon View" are the best-known VDI solutions. Depending on the supplier, the connection broker may have additional functions, such as a web interface that can create secure (SSL) connections to remote desktops, Directory Services integration, Full USB support, support for various display protocols and integration with Remote Desktop Services Session Host (formerly RDSH). Depending on the rules, it is possible to execute applications centrally on a server-hosted VDI or on a terminal server.



Functions of this object are:

- Server Hosted Applications and desktops, the grey window with Application logo.
- The 'compass', who determines which user will get access to which applications or desktops, both persistent and non-persistent.

4.7 APPLICATION VIRTUALIZATION

Through application virtualization, Microsoft Windows applications can be used without changing the local operating system or installing the application software at a particular work place. In other words; the application can be executed as if it had been installed locally and can save data and print without the need for any modifications to the local client. Resources such as the CPU, memory, hard disk and network card take care of the execution of these applications.
Application streaming and virtualization can make applications available to desktops, laptops, server-hosted VDIs and Remote Desktop Services Session Host (TS) platforms. The applications are executed on a "client" platform, without needing to modify the platform.

The advantages of application virtualization include: installation, upgrade, roll-back, delivery speed and the ease of application support and management). Installation of applications is no longer necessary, eliminating the possibility of conflicts. The result is a dynamic application delivery infrastructure. Application streaming and virtualization solutions include: Cameyo, Citrix (XenApp) application streaming, Microsoft App-V, Symantec Workspace Virtualization, Spoon and VMware ThinApp. More unique information about application virtualization can be found here.

4.8 OS PROVISIONING

OS Provisioning, or Machine Based Imaging, allows workstations to boot up and run from a central image. A single image can be used simultaneously by multiple workstations. The advantage of this is that complete operating systems, including applications and agents, can be made available quickly and securely. It's possible to make a single image available to multiple VDIs, RDS, Client Side Virtualization and physical desktop environments without causing conflicts. This allows the OS to be upgraded or rolled back quickly, simply, and without significant risks. When virtual desktops use OS streaming, (valuable) storage is saved and the management of virtual desktops becomes relatively simple. This means that virtual or physical machines using OS Provisioning can become - stateless devices. Citrix Provisioning Services and Machine Creation Services, part of the XenDesktop family, Doubletake Flex, VMware Mirage, Dell/Wyse Streaming Manager (WSM), Unidesk and the VMware View Composer are solutions that facilitate OS Provisioning.

4.9 SERVER-HOSTED DESKTOP VIRTUALIZATION (VDI)

A Server-Hosted Virtual Desktop Infrastructure (VDI) is a dedicated remote desktop solution providing remote access to Windows XP/Vista/Win7/Win8/Server2008/Server2012 or Linux desktops. The virtual machines are running from within the data center. The virtual infrastructure increases the system's independence, availability and manageability. The implementation of Server-Hosted VDIs means that desktops are no longer bound to a location or end-user appliance. Each user can have their own unique, personalized, fully independent work place. Programs run and data is processed and stored on a centralized personal desktop. The information is sent to the client screen via a remote display protocol such as Microsoft RDP/RemoteFX, Citrix ICA/HDX, Teradici/VMware "PC-over-IP", SPICE or VNC. The protocol used for displaying the correct information depends on the operating system, bandwidth, the type of application, and the technical facilities. As with other desktop delivery solutions, VDI consists of various infrastructure components that facilitate management, load balancing, session control and secure access to virtual machines. Microsoft, Citrix, Dell/Quest, Oracle, Virtual Bridges, RedHat and VMware are all important suppliers within the server-hosted VDI segment.

4.10 VDI WITH GPU ACCELERATION

"Graphical Processor Unit (GPU) acceleration" functionality can be added to the server-hosted VDI solution. It provides each (virtual) machine with graphic performance to run multimedia, 2D/3D, NextGen and CAD/CAM applications.
Display data is presented to the client device via an optimized remote display protocol. To ensure end-users experience the best possible performance, the bandwidth, latency, or local (software) components have to meet extra requirements.

4.11 SESSION VIRTUALIZATION (TS)

With session virtualization every user has his or her unique terminal server *session*. Session Virtualization, also known as Terminal Services, is a solution for the remote access to desktops and applications that are run on a terminal server in a data center. Access to the desktop or application is not tied to a location or end-user machine, and programs are executed centrally on the terminal server.
The data appears on the client screen through a remote display protocol such as Microsoft RDP/RemoteFX or Citrix ICA/HDX. Remote Desktop Services consists of various infrastructure components for management, load balancing, session control and support. It has the advantage that applications are made available quickly and securely, the TCO is low, and applications can be accessed irrespective of location or work place. Suppliers of Remote Desktop Services Session Host (TS) include Citrix, Ericom, Microsoft and Dell/Quest.

4.12 CLIENT-SIDE VIRTUALIZATION

Client-side Virtualization is a dedicated local desktop where the virtual machines run locally on the client device. The hypervisor ensures that each virtual machine is hardware-independent, and makes it possible to simultaneously use a number of virtual machines at the same workstation. The hypervisor plays an essential part in client-side VDI solutions while the management portion handles synchronization, policy, enforcement and management insights.
The two types of Client-side Desktop Virtualization solution are:

- **Type 2 - 'client hosted' hypervisor** is installed and runs as an application on the operating system (be that Windows, Mac OS X or Linux) of the end device.
  (Examples are: Citrix DesktopPlayer for Mac, Microsoft Virtual PC, MED-V, MokaFive, Parallels Desktop, Oracle VirtualBox, VMware Fusion/Workstation and VMware View Client with Local Mode)
- **Type 1 - 'bare-metal' client hypervisor** acts as the device's base operating system and must be installed before other operating systems.
  (Examples are: Citrix XenClient, Citrix XenClient Enterprise - formerly Virtual Computer NxTop - and Windows 8 Hyper-V)

The main differences between type#1 and type#2 hypervisors are hardware support, performance, manageability and end-user experience.

4.13 WORKSPACE AGGREGATION

The term Workspace Aggregator is used to describe software that unifies the delivery of multiple application or desktop types such as:

- Native mobile applications;
- Software as a Service (SaaS) applications;
- Mobile web applications;
- Windows Applications via application virtualization or installation;
- Desktops, local, server Hosted Virtual Desktops (VDI) or published Desktops in SBC.

A workspace aggregator also evaluates the user's device to determine which applications are available for this user on this particular device and at this particular time (context-aware access). Next to application delivery, workspace aggregators provide secure file data access from a broad range of devices. A workspace aggregator simplifies the deployment and life cycle management of applications. As the single point of access, (de)provisioning, auditing and monitoring is easily accomplished through security rules and policy enforcement. Many workspace aggregators also provide Single Sign On capabilities to applications. 'Workspace aggregation' is a strategic function in the tomorrow's workspace that is independent from hardware and is OS and browser neutral. Workspace aggregators will mature and become more and more complete over time.

4.14 CLIENT MANAGEMENT

Any self-respecting professional IT organization is bound to use a Client Management solution to facilitate tasks such as OS deployment, patch management, application and client deployment, asset management, service desk integration, and remote control.

Example client management systems are Altiris/Symantec Client Management, IBM BigFix, LANdesk Client Management , Microsoft System Center Configuration Manager (ConfigMgr/SCCM) and Novell ZENworks Configuration Management (ZCM).

Functions of Client Management (in the context of Application and Desktop Delivery) are:

- Deliver and manage Windows applications
- Deliver and manage Windows Operating systems

4.15 VENDOR MATRIX, WHO DELIVERS WHAT

This whitepaper mentions a variety of vendors and products. An overview is shown below:

Vendor	Product	Solution
Citrix	XenDesktop	VDI
Citrix	VDI-in-a-Box	VDI
Ericom	PowerTerm WebConnect	VDI
Microsoft	VDI with RemoteFX	VDI
RedHat	Enterprise Desktop Virtualization	VDI
Dell/Quest	vWorkspace	VDI
Virtual Bridges	VERDE	VDI
VMware	View	VDI
Ericom	RDP/Blaze	Remote Display Protocol
Citrix	HDX-ICA	Remote Display Protocol
HP	RGS	Remote Display Protocol
Microsoft	RemoteFX/RDP	Remote Display Protocol
Dell/Quest	EOP/RDP	Remote Display Protocol
Oracle	ALP	Remote Display Protocol
Virtual Bridges	SPICE	Remote Display Protocol
VMware/Teradici	PCoverIP	Remote Display Protocol
Teradici	PC over IP	SH- Physical Desktops
Ericom	PowerTerm WebConnect	SH- Physical Desktops
HP	Remote Graphics Software	SH- Physical Desktops
Citrix	XenDesktop HDX3D Pro	SH- Physical Desktops
VMware	View	SH- Physical Desktops
Citrix	XenClient	CSV, Baremetal
Citrix	XenClient Enterprise	CSV, Baremetal
Microsoft	Windows 8 Client Hyper-V	CSV, Baremetal
Virtual Bridges	LEAF	CSV, Baremetal
Citrix	DesktopPlayer for Mac	CSV
Microsoft	MED-V (MDOP)	CSV
VMware	Player/Fusion/Workstation/View	CSV
Bromium	vSentry	CSV, Security
Double Take	Flex	OS Provisioning
Citrix	Provisioning Services / MCS	OS Provisioning
Citrix	Personal vDisk (former RingCube)	OS Provisioning++
Quest/Dell	HyperDeploy	OS Provisioning
VMware	View Composer	OS Provisioning
VMware	Mirage	OS Provisioning++
Unidesk	Unidesk	OS Provisioning++
Virtual Bridges	Dynamic Gold Imaging	OS Provisioning
Dell/Wyse	Streaming Manager (WSM)	OS Provisioning
Microsoft	Windows Server 2008R2/2012	Session Virtualization
Citrix	XenApp	Session Virtualization
Dell/Quest	vWorkspace	Session Virtualization

Vendor	Product	Solution
Cisco	ASA	Secure Access
Citrix	Netscaler Gateway	Secure Access
Ericom	Ericom Secure Gateway	Secure Access
Microsoft	Unified Access Gateway	Secure Access
Juniper	SA	Secure Access
VMware	View	Secure Access
Citrix	Application Streaming	Application virtualization
Cameyo	Cameyo	Application virtualization
Microsoft	App-V	Application virtualization
Symantec	Workspace Virtualization	Application virtualization
Spoon	Spoon	Application virtualization
VMware	ThinApp	Application virtualization
Fiberlink	MaaS360	Client Management
IBM	BigFix	Client Management
LANDesk	Client Management Suite	Client Management
Microsoft	System Center Config Manager	Client Management
Novell	ZenWorks Configuration Mgr	Client Management
Symantec	Client Management Suite	Client Management
RES	Automation Manager	RunBook Automation
Citrix	XenMobile	Workspace Aggregator
VMware	Horizon Suite	Workspace Aggregator
Centrix	Workspace Universal	Workspace Aggregator
Framehawk	Framehawk	Workspace Aggregator
Airwatch	Enterprise Mobility Mgmt Suite	Mobile Application
Appsense	MobileNow	Mobile Application
Cisco	Meraki	Mobile Application
Citrix	XenMobile	Mobile Application
Fiberlink	MaaS360	Mobile Application
Good	For Enterprise	Mobile Application
Microsoft	Windows Intune	Mobile Application
MobileIron	Advanced Management	Mobile Application
Symantec	Mobile Management Suite	Mobile Application
VMware	Horizon Mobile	Mobile Application

Table 1, Application and Desktop Delivery overview of solution area, products and vendors.

5. SECURITY

Security is probably the biggest driver to think about Enterprise Mobility Management (EMM) in the first place. After all: why would we want to centrally manage devices that are meant to be used individually and are designed to reach the highest level of user friendliness? It is because these devices will be used to access our confidential information. Confidentiality is one of the three pillars of information security.

So how do we secure mobile devices, to an extent that we truly keep in control over our dearest bytes?

5.1 MAIN CHALLENGES

The three main challenges for Security in Enterprise Mobility Management:

5.1.1 Mobility

First and most important is the simple fact that mobile devices, smartphones, tablets and laptops will typically be used outside the boundaries of the corporate network. In order to keep track of their usage, and system health, it is essential to design security controls that are effective regardless the location of a device. However, not only need the controls to be in effect, they need to be in continuous control as well.

In the event a mobile device is lost or stolen, it's vital the finder (or thief) cannot get access to the data and applications running on it. Corporate data for example stored in a user's email inbox, synchronized to the device can easily outweigh the value of the device itself.

Furthermore if a device is used outside of the corporate network (e.g. an airport), it will be connected to unknown (untrusted) networks with probably little network security components in place. In such situations, it needs protection from exploitation locally that matches the level of security that is applied to the corporate network. Especially firewalling, intrusion prevention and patch management are security controls that need attention.

5.1.2 Variety

There are many different types of different mobile devices from laptops to smartphones and tablets. In addition different Operation Systems and versions used. These differences make applying security measures on some configurations difficult and in some cases impossible.

Without laying out all the technical details, organizations that want to be in control over their security, simply first need to define what security controls need to be implemented. Only afterwards, it is possible to build a list of supported devices and operating systems that can comply with the defined level of security. Especially when Bring-Your-Own-Device (BYOD) is part of the EMM strategy.

5.1.3 Ownership

Bring-Your-Own-Device (BYOD) is often part of an EMM strategy. In this scenario, devices are owned and maintained by the user. Security often boils down to trust, and in this case, the

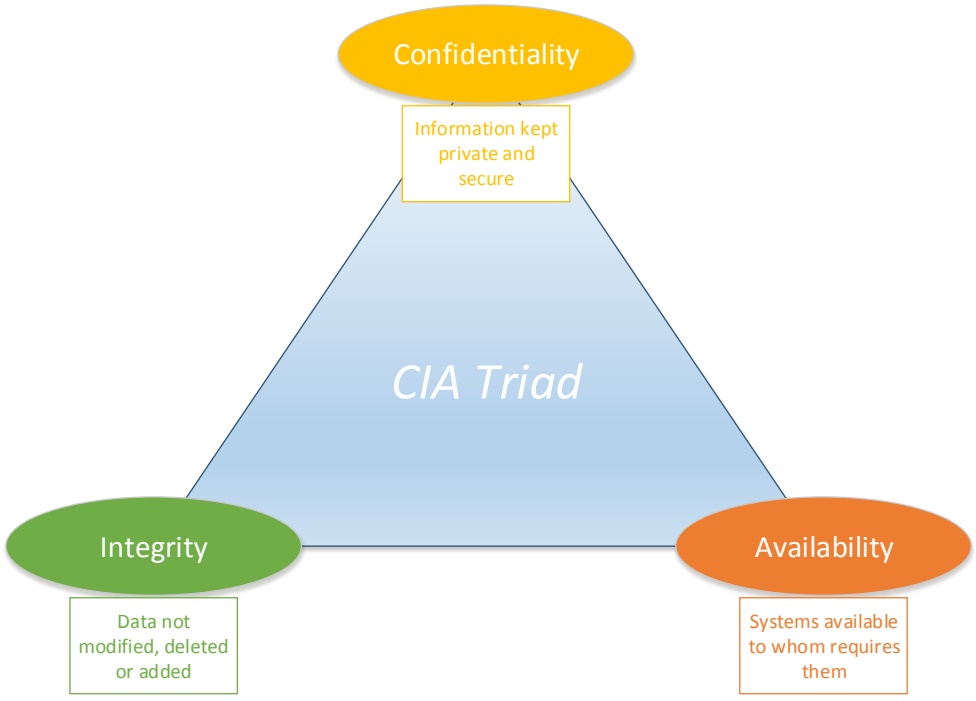
question arises: “Can we trust the owner of the device to properly manage it”? Probably that is not the case, which indicates that such a device might as well be compromised by a cybercriminal at any given time. Letting such devices connect to the corporate network therefore poses a certain risk.

Devices that are not owned and maintained by the organization should always be placed in a separate part of the network. From there, only the required network connectivity to the corporate network can be allowed and deeply inspected for anomalies.

Another result of shifted ownership is that changes to the device (installation of software, deletion of files) cannot be initiated by the organization without prior consent of the user. Addressing this requires the company to have a proper policy signed by all users that access corporate data from their own device.

5.2 THE GOAL

The goal of applying security to Enterprise Mobility Management is to guarantee **confidentiality**, **integrity** and **availability** of corporate **data**, in order to maintain continuity of information and systems and limit the potential damage caused by security incidents to a certain defined level. The three general pillars of information security together form the CIA Triad:



When applied specifically to EMM, these three elements can be translated as follows:

- **Confidentiality**: When data is stored on, or can be accessed from mobile devices, how do we ensure that only authorized users are able to view confidential information?
- **Integrity**: How do we make sure that mobile devices, and the processes and users on them can be prevented from making inappropriate changes to corporate data?
- **Availability**: How do we support mobile users as they require access to corporate data and systems?

5.3 VISION

EMM and specifically Mobile Device Management is often viewed as a separate or subpart of IT Security management. Moving forward we believe that mobile devices (regardless of who owns them or what form-factor) will form the majority of corporate devices. These are the "next generation endpoint devices" and should be an integrated part of the overall corporate IT Security strategy along with traditional desktops.

In order to provide strong preventive security to this new breed of endpoints, Risk Management should be applied. To achieve this, consider the following:

1. Layout a good security policy that is supports business goals.
2. Find out and prioritize what assets exist within the (wide area) network.
3. Know which vulnerabilities are applicable to your systems and to what level they pose an actual risk to your organization (Risk = Probability x Expected Loss).
4. Apply security as counter-measures to the risks that need fixing.
5. Maintain an overall insight in status and effectiveness of security measures.

6. MOBILE IT STRATEGY

The growing reality of Consumerization of IT and the increased use of personal mobile devices at work is causing many IT organizations to re-evaluate traditional IT operations, support, and management methods. A good strategy for how to support these users is important to prevent unwanted challenges.

We see many organizations primarily focusing on **features**, **products** and **vendors** and lacking a clear and profound overall vision and strategy. This approach is not good or bad it depends on what the goal of the organization is. When the organization needs a point solution, the various vendors and corresponding products can help to solve this issue and fill-in the demands.

When the organization is investigating possibilities, advantages, use cases and functionality of Enterprise Mobility Management", a profound vision and strategy should be in place. The following *discussions* and corresponding *topics* should be part of Mobile IT strategy:

Devices

- What **types of device** should be covered e.g. smartphones, tablets , laptops?
- What type of **operating systems** and devices need to be supported?
- **Who owns the device**?
- Do you allow personal devices (**BYOD**)
    - What happens to uses personal applications and data?
    - What level of support should be provided for personal devices?
- Is **Company-Owned Personally Enabled devices**? (COPE) an option?
- Is the Mobile IT strategy focused on **Device**, **Application** or Information/**Data** management?
- With personal devices, are users **self-supporting**?
- What happens with lost or stolen devices - can the data be wiped – full or selective?

Applications

- What is your '**Application delivery' strategy**? Do you want to deliver Windows applications and desktops, native rich mobile apps, classic web/SaaS applications and/or HTML5 based applications to various devices?
- What type of **applications** do users need to be more **productive**? E-mail, browser, fileSync, productivity suites, Line of Business Applications?
- Are you planning to **develop** your own mobile apps (in-house or through ISV)?
- Do you want to support internal **web applications** to mobile devices?
- Will users accept a **third-party email client** for corporate email?
- Is Unified Communications part of the MobileIT strategy?
- What is the (business) applications **vendor support** policy for EMM?

Data Management

- Who **owns** the data, if corporate data is stored on the user's personal device?

- What **information** do users want to access on their mobile devices? Do you want to separate personal and corporate information on the device?
- Are there any **regulations** about storing **information** on the device?
- Do you want to prevent users sharing **corporate** data with personal applications?
- Do you need **encryption** on the device or on specific content?

Secure Access and Networking

- What is the **impact** of **Secure Access and Secure Networking** solutions on mobile devices while connecting to hosted apps or desktops? What will the **user experience** be like with these secure access solutions?
- What are the performance, authentication, security, manageability and availability requirements for Secure Access and Networking?
- Do you want to give devices and/or applications Secure Access to corporate resources? Do the current Secure Access solutions meet the requirements? What will the User Experience be like?
- Do you need 2-factor authentication for application delivery? If so, does the solution integrate in the Enterprise Mobility Management solution?

Policies and regulations

- Do you have a mail / **messaging** security policy?
- Do you have a **data** security policy?
- Is encryption of email attachments secure enough to comply with your security policy?
- Do you have a need to block certain mobile device capabilities, like the camera or specific software?
- Are specific security or **compliance** regulations set for your region?
- What information do you want/need to **monitor** from the device?

Generic

- Who is the **owner** of the MobileIT **strategy**? What are the goals?
- What is the **business-case?** What do you expect as a ROI?
- What do you want to **achieve,** a **business enabler**, overall cost of ownership (**TCO**) and **cost reducer**?
- Do you understand the EMM vendor vision, strategy and roadmap?
- Is there a **validated design** for the Enterprise Mobility Management solution?
- Do you want the Enterprise Mobility Management solution as a **public cloud** service or hosted and maintained in your own **private** datacenter?
- Is the IT department able to **adopt** the technology with right **knowledge** and **skills**? What subject matter experts are needed to get and keep the EMM solution up and running in production environment? Is this **expertise** available? Who has **overview** of the complete EMM solution stack?
- Is the EMM vendor a **financially healthy** organization? Is this important in evaluation of the vendor and the solution?
- Is there a huge **ecosystem** with **partners**, **consultancy**, training and **education** around the EMM solution? Is this important for you?

- Is C-level management, Security, Networking, HR, Application Delivery, Workspace Support and overall the business consumer involved in the MobileIT strategy?
- There is not a standard for Mobile Application Management solutions, using MAM solutions for application delivery is a long-term commitment.
- How do you make sure the solution meets the **User Experience** so the solution will be adopted?

***Bottom Line: Mobile IT strategy is teamwork. Success** = **Vision** x **Execution** x **Adoption**.*

7. ENTERPRISE MOBILITY MANAGEMENT

7.1 INTRODUCTION

The term “Enterprise Mobility Management” is used to describe solutions to securely manage devices, applications and data. There are numerous products / solutions available, each using a slightly different approach to support mobility.

This chapter describes the following:

- Mobile Device Management;
- Mobile Application Management;
- Mobile Information Management;
- Mobile Expense Management;
- Secure e-mail;
- Secure Data;
- Secure Web browsers.

7.2 MOBILE DEVICE MANAGEMENT

Mobile Device Management (MDM) solutions are primarily a policy and configuration management tool for mobile handheld devices such as smartphone and tablets.

MDM is aimed at managing the device. After a device is “enrolled” to a MDM server, a configuration profile or MDM application is installed on the device. This contains specific settings for this device. In addition – and this is important for BYOD initiatives – the IT department is able to monitor activity on the device (like installed applications, message flows) and enforce restrictions on the device (like passcodes, application blacklisting).

Using policies, organizations have a way to deploy and remove applications on the mobile device. These policies can also contain rules to specify which other (personal) applications are specifically allowed or denied on the devices. Mobile Device Management also provides ways to provision mobile devices with a secure configuration such as certificates and WIFI connections. When devices fall out of scope of IT management, Mobile Device Management solutions are able to completely or selectively wipe the mobile device.

In general, the following list contains the features delivered by the MDM solutions on the market today:

- Provisioning
- Policy enforcement
- Asset management
- Administration
- Reporting

With some exceptions, Mobile Device Management is performed over-the-air. This allows the IT department to control the device independent from its location – after all, mobile devices are *considered* ‘always-online’.

Mobile Device Management introduces some difficulties. Mobile operating systems are designed with security in mind. Applications do not have access outside their own 'container', whether it is on Apple iOS, Google Android, BlackBerry or Microsoft Windows Phone. Mobile operating systems are equipped with management API's. These API's determine the capabilities of the MDM solution. If the mobile OS does not support a particular restriction (e.g. "block the camera") a MDM product simply cannot enforce this restriction. Therefore, in general, all MDM vendors have access to the same API's and are able to deliver the exact same functionality on the management piece.

To make things a little bit more complex, there are differences between iOS and Android, and between the different versions of Android. Again, the mobile OS determines the capabilities, so specific features may be possible on iOS but not on Android (and vice-versa). As Android is open-sourced, OEMs are allowed to modify the operating system to fit their needs and extend the management API's. Samsung SAFE (Samsung Approved For Enterprise) is the best example here. SAFE adds a lot of management features to Android but is obviously limited to Samsung devices only. The fragmentation within the Android releases makes it hard to choose the right management solution!

As mentioned before, the MDM vendors provide largely the same features, as they are all dependent on the API's available within the Mobile operating systems. However, there are some differences too. The most important differences are found on document/file sharing, delivery model, containerization, application delivery and management/reporting features and ease-of-use.

While some companies think about MDM products as THE solution for their mobility challenges, keep the following in mind:

- MDM manages the device
- Users generally don't want a locked-down device, certainly not when it's their own device (BYOD)
- MDM solutions are limited by the management API's of the mobile operating systems
- Take the management differences between the mobile operating systems into account

Ask yourself the question - "Is Mobile Device Management the way to go to support BYOD initiatives?" In most cases the answer will be - No! ... "No way will I let IT tell me what to do with my OWN device or configure complex password policies on MY device.

However, there are use cases for MDM products such as healthcare, transportation companies, education etc where mobile devices can be used for specific tasks (a bit like a kiosk-mode PC is used today). In these use cases a locked-down device works very well.

7.3 Mobile Application Management

Mobile Application Management provides a way to securely deliver native applications to employee-owned, unmanaged and insecure mobile devices. Applications are 'wrapped' or 'containerized' to allow delivery of the application using a Corporate Application Store. In addition, data and information is stored within the application container, allowing IT to revoke the application and selectively wipe the corresponding data, leaving the user's personal information intact.

With Mobile Application Management, it is no longer necessary to control/manage the device because policies can be applied to specific (corporate) applications. The user's personal applications can be used next to the secured corporate apps, without any limitation and without letting IT control the device. This is a great way to support BYOD initiatives! The user is not restricted to a certain type of device. Passlocks on the device are not needed; this also applies for whitelisting/blacklisting applications. Posting a new status on Facebook or Twitter, taking a picture of your kids will not confront the user with restrictions determined by their company.

This changes when the user starts a corporate app. By placing policies on the applications, IT can determine that the application is allowed to start under specific conditions – like, but not limited to, Wifi connection or a 13-character domain password. In addition, any information that is stored by this corporate app(s) can be encrypted and selectively wiped without touching the user's personal applications, documents and pictures.

However, Mobile Application Management only works for applications that are delivered by the MAM solution. If a user downloads apps from the public application stores – Apple App Store or Google Playstore – these applications cannot be managed by MAM. This is due to the closed mobile operating systems; a MAM agent cannot control other applications because this is prohibited by the operating system.

The solution is to deliver applications from a corporate or private application store. All MAM vendors provide a way to deliver your own mobile applications. Dependent on the supported methods from the MAM vendor, the application delivery process contains a step where you 'wrap' your application or build it with a specific Software Development Kit (SDK). This enables the administrator to set policy controls on the application. Please refer to chapter 3.3.4 for a summarization for the differences between these approaches.

Mobile Application Management seems the way to go to support BYOD. Security policies which apply just to corporate apps and not to employee-owned devices are often a more acceptable approach for users.

However, MAM introduces some new challenges. At this moment, there is no common standard to wrap of sign applications. Whether you can use 'app wrapping' or an SDK is determined by which approach is supported by your MAM product AND only works for that MAM product. Consider this when choosing your best solution!

7.4 Mobile Information Management

With MIM, the focus is on managing the data / information. Using policies, the IT department can control access, encryption and prevent data loss, no matter which application is used to access the data. After all, using Mobile Application Management, access to the information is through applications. The user however is not free to choose whatever application he likes to use. Mobile Information Management is probably the best Fit to support Consumerization of IT.

There are no true MIM solutions available on the market today, as this is not possible due to the closed architecture of mobile operating systems. Enforcement of secure information storage on mobile devices is possible using MAM techniques in addition with filesync applications, secure mail and secure webbrowsers. These topics are explained in chapter 7.6 and up.

7.5 MOBILE EXPENSE MANAGEMENT

Mobile Expense Management can support organizations ability to reduce or limit costs for data roaming. With MEM solutions, data plan management provides insights into use and warnings can be sent to users when certain thresholds are reached. Mobile Expense Management is a good fit for company owned devices.

7.6 SECURE E-MAIL

In general, E-mail and calendaring are the killer features on mobile devices. The mobile device is a perfect form factor to read e-mail, send (short) replies and make appointments using the calendaring app or organize your contacts. However, this information can contain sensitive company information, especially with email messages and the inevitable attachments.

Secure e-mail is possible in different ways, and with different apps. Some methods work with the built-in (native) app. This typically gives the best user experience. Other methods use a third-party application to separate the corporate mail, calendar and contacts.

Probably the easiest (and most limited) method is use of Microsoft Exchange Server with Exchange Active Sync (EAS) policies. With EAS you can enforce a pass lock – and some more - on the device. This works well with the native mail application. However, in many cases this is not enough.

Another method is to encrypt the attachments as soon as they're delivered to the mobile device. The only way to decrypt the attachment is to open it using a managed application, which triggers the authentication methods and policy rules to prevent unauthorized usage. This only works for attachments, any information in the message (like text) is insecure and can be forwarded to anyone or copy/pasted to another (unmanaged) application.

The last method is to use a third-party email clients such as Citrix WorxMail (iOS and Android) or Nitrodesk Touchdown (iOS and Android). The email client is generally delivery using Mobile Application Management vendors and can be as secure as any other managed application. The third-party email client is used solely for corporate email. Using MAM policies, the IT department can control which applications are able to open attachments. Because the third-party email client is contained in a sandbox, encryption is possible for email messages AND attachments.

Many users understandably like / prefer the built-in native mail app on their device. This is not most secure form of e-mail. A key question is – will users be willing to step away from the native app for their corporate mail and use a different and much more secure alternative e-mail app? Third-party email clients try to make it more attractive to use their app by providing features that native clients lack. This may be as simple as showing the week numbers in the calendar app, or inserting/reading attachments to appointments or see free/busy information when scheduling an appointment. Whether this is enough is up to your users.

Most MAM vendors deliver their own third-party email app.

7.7 SECURE DATA, ENTERPRISE FILESYNC

Dropbox (and others) are widely used because it is intuitive and easy to use. It enables users to have access to and store documents/file on any device they use – desktops and mobile devices. As most of these (free) file sync vendors store the data in the Cloud, companies are not keen to use this form of data access. Today, numerous products provide similar functionality with on-premises storage. In addition, they provide mobile file sync applications for mobile devices.

These mobile FileSync applications are delivered using the same techniques as the third-party email app or any other mobile application. Mobile Application Management (again) provides the architecture and tools to deliver a FileSync app and configure policies to restrict/allow access and encryption – for both syncing and storage. This also allows the IT department to control which applications the user is allowed to use to access this data. To prevent data leakage, it might be obvious to allow only managed mobile apps. Most MAM vendors deliver their own mobile file sync app and infrastructure. The FileSync infrastructure, authentication and data storage can be a SaaS or on-premises solution.

7.8 SECURE WEB BROWSERS

The methods mentioned earlier to access data have all relied on mobile apps. However, a growing percentage of enterprise applications are already available as web-architected applications – on-premises or as SaaS from the Cloud. Secure web browsers, again delivered as a managed mobile app, provide secure access to internal resources. Using the MAM techniques to secure access to the application, internal web resources are accessible from mobile devices. This is enabled by using some sort of VPN tunneling techniques – the exact implementation differs from vendor to vendor. A great advantage with this solution is that it's not necessary to allow direct access from the internet to internal resources. The server(s) needed for the MAM deployment is responsible for name resolution, URL rewriting and (secure) access to internal webservers. Most MAM vendors deliver the own secure web browser app and infrastructure.

8. VENDORS AND THEIR EMM SOLUTIONS

8.1 INTRODUCTION

To give an overview of the major players in the Enterprise Mobility Management (EMM) space, a number of solutions are described in this chapter (sorted alphabetically by vendor). The goal is to enable a better understanding of the Enterprise Mobility Management space from a vendor perspective – in their own words.

Note: The vendor solution descriptions are provided by the vendors. However, we have attempted to remove the marketing fluff wherever possible.

8.2 AIRWATCH ENTERPRISE MOBILITY MANAGEMENT SUITE

INTRODUCTION

Founded in 2003, AirWatch is a leading provider of enterprise mobility management (EMM) solutions. Their mobility platform encompasses Mobile Device Management (MDM), Mobile Application Management (MAM), Mobile Content Management (MCM), Bring Your Own Device (BYOD), Multi-User Management and much more. AirWatch employs over 1,200 people, with more than 400 in research and development – the largest in the space. The AirWatch leadership and development teams designed their software with the goal of supporting the most scaled, most global and most security-conscious organizations in the world.

AirWatch has more than 6,500 customers with deployments in over 150 countries in the education, finance, government, healthcare, retail and transportation industries. International customer growth has continued to expand with six global offices in Atlanta, Washington D.C., United Kingdom, Australia, India and a presence in Singapore.

The Airwatch Enterprise Mobility Management Suite consists of the following solutions:

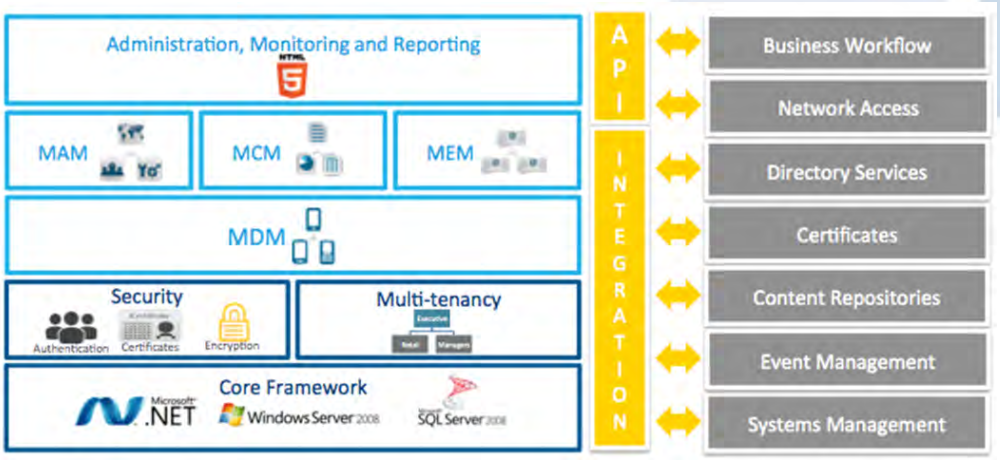
- **Mobile Security** - ensure your enterprise mobility deployment is secure and corporate information is protected with end-to-end security that extends to users, devices, applications, content, data, email and networks. AirWatch provides real-time device details and continuous compliance monitoring to ensure your users, devices and corporate data are secure.
- **Mobile Device Management** - enable businesses to address challenges associated with the mobile devices by taking complex issues and creating simplified, comprehensive and user-friendly solutions without sacrificing security. AirWatch provides the ability to quickly enroll devices in your enterprise environment, configure and update device settings over-the-air, enforce security policies and compliance, secure mobile access to corporate resources, and remotely lock and wipe managed devices. With AirWatch, you can manage a diverse fleet of Android, Apple iOS, BlackBerry, Mac OS, Symbian, Windows Mobile and Windows Phone devices from a single console.
- **Mobile Application Management** - addresses the challenge of acquiring, distributing, securing, and tracking mobile applications. Easily manage internal, public and purchased apps across corporate-owned, corporate-shared and employee-owned devices from one central console.

- **Mobile Content Management** - secure distribution and mobile access to documents with AirWatch Secure Content Locker™ (SCL). With SCL, you can protect sensitive content in a corporate container, and provide employees with a central point to securely access the latest sales presentation, board book or financial report from their mobile device.
- **Mobile Email Management** - deliver comprehensive security for your corporate email infrastructure. With AirWatch, you can control mobile devices accessing email, prevent data loss, encrypt sensitive data and enforce advanced compliance policies. AirWatch supports native email clients, containers, enterprise services and cloud-based clients.
- **Bring Your Own Device** - AirWatch enables unprecedented choices over the types of devices you deploy and the device ownership models you support, without compromising the security and management of your mobile fleet. AirWatch provides a flexible model for asset management, policy enforcement and distribution of profiles and apps based on device ownership.
- **Multi-User Management** - AirWatch helps companies across multiple industries address the challenges of multi-user device management by providing the most innovative multi-user management solution. AirWatch can help you meet enterprise security and management requirements for corporate devices while providing the personalized experiences that users demand.

ARCHITECTURE

AirWatch scales to support deployments of hundreds to thousands of devices through a robust architecture that is fully configurable according to their customers' environments and requirements. AirWatch's solution is built on industry standard technology, making it easy to manage alongside existing enterprise applications. AirWatch can be deployed in a highly available environment and fully supports disaster recovery configurations to minimize downtime. AirWatch's solution key features include:

- **Scalability** – Highly scalable architecture designed to easily support from 10 to over 100,000 devices and to seamlessly scale as deployments grow
- **Multi-tenancy** – Multi-tenant structure that allows organizations to absorb fragmentation within their corporate infrastructures (e.g., disconnect AD servers, forests, domains, locations) into a single instance of AirWatch
- **Configurability** – Designed around the componentization of core functions, allowing for the deployment of the software specific to varied environment and architecture requirements
- **High Availability** – Supports using network load balancers, VM HA technologies, and server clustering to provide a full highly available solution from the application servers to the SQL database
- **Disaster Recovery** – Can be set up in a remote data center to support disaster recovery configurations
- **Flexible Deployments** – Available in cloud or on-premises hosting environments



Regardless of the deployment type, AirWatch provides deep integration with on-premises corporate resources.

- **Directory Services** – Integrate with AD/LDAP for authentication and group membership
- **Certificates and PKI** – Integrate to Microsoft CA, CA, or SCEP certificate services providers, such as MSCEP and VeriSign
    - Automatically distribute certificates to devices and configure access to resources without requiring any user interaction
    - Renew certificates and view soon-expiring certificates
    - Revoke certificates through a certificate management dashboard that provides full visibility into the status of configured certificates
- **Email Infrastructure** –
    - Proxy – Exchange 2007 or lower, Lotus Domino or Lotus Traveler, Novell GroupWise, Beehive and other EAS
    - PowerShell – Exchange 2010, Office 365/BPOS
    - Google – Google Apps for Business
- **Corporate Networks** – Configure Wi-Fi and VPN network settings
- **File Systems** – Integrate directly with existing file systems, including SharePoint, file servers and networks shares
- **Internal Apps (SDK)** – Build business apps that leverage core security, integration and management capabilities
- **APIs** – Integrate with existing IT infrastructures and third-party applications
- **Security Information and Event Management (SIEM)** – Integrates with SIEM solutions for enhanced logging of events occurring in the console

LICENSING

AirWatch licensing is device based and available in two licensing models. For Subscription licenses, there are no upfront costs or long-term commitments, and flexible contract terms allow customers to pay month-to-month. Customers can also choose to make an initial investment and purchase perpetual licenses.

- **Subscription License** – Monthly fee per device, maintenance included
- **Perpetual License** – One-time fee per device, maintenance 20% annual fee

Deployment Options

AirWatch provides two options for deploying their solutions – in the AirWatch Cloud or on-premises. Regardless of the deployment model, AirWatch provides exactly the same functionality.

AirWatch Cloud

The AirWatch solution is available in both a shared hosted and dedicated hosted environment and is easily accessible over the internet. In one single instance of the software, AirWatch is able to deliver a secure and scalable cloud-based solution comparable to an on-premises deployment.

Cloud Advantages

- Scales to support 1 to 100,000+ devices
- Quick to deploy and requires minimal effort
- No significant investment in technology
- Maintenance and upgrades handled by AirWatch
- Option to transfer to on-premises deployment

On-Premises

AirWatch can be deployed, managed and maintained fully on-premises providing behind the corporate firewall security, or as a dedicated software appliance. Whether you are using dedicated hardware or virtualized environments, AirWatch delivers flexibility, scalability and control.

On-Premises Advantages

- Scales to support 1 to 100,000+ devices
- Tight integration with enterprise services
- Complete control over hardware and software
- No transmission and storage of data off site

8.3 AppSense EMM Suite

Introduction

The AppSense Enterprise Mobility Management Suite offers end-to-end security for mobile devices, applications, data, email and content. The suite is comprised of two solutions: AppSense MobileNow (providing mobile application and device management) and AppSense DataNow (offering File Sync & Share and secure anywhere data access).

AppSense MobileNow

AppSense MobileNow is the first and only on-demand enterprise mobility solution that secures devices, apps, and data in real-time; providing the end to end security and control that IT needs while enabling the freedom of choice that users demand MobileNow provides the full suite of required features and functionality for truly comprehensive enterprise mobility management:

- **Mobile Device Management (MDM)**. MobileNow provides full-featured, comprehensive MDM functionality that can be deployed seamlessly with or independent of the rest of the MobileNow suite. It enables IT to exercise a wide range of device controls – from completely open to highly secure – and enforce device-level policies from a re-

mote console without ever having to physically handle an end-user's device. Once IT configures the administrator console, end-users are just a single click away from accessing all their business information from their mobile device. With robust MDM policies, IT can provision an end-user 100% over-the-air, implement and manage comprehensive device policies with full auditing, and remotely configure devices for Wi-Fi, VPN, email and other access.

- **Mobile Application Management (MAM)**. MobileNow's MAM functionality enables complete application and data lifecycle management – from provisioning until end-of-life – without modifying application code or the device operating system. From a central console, IT can define, set and push fine-grained application, data, compliance and even location policies without ever touching an end-user's device. IT can segregate personal from business applications and data, whether built in-house or by third parties, resulting in complete end-user satisfaction. Moreover, MobileNow ensures complete security by encrypting all business application data with AES256 encryption algorithm, unlike first generation BYOD solutions that deploy weak device-level encryption schemes.
- **Secure Native & Third-Party e-Mail**. MobileNow provides two options for corporate email access. The first option is a secure and fully native email client that allows business email to exist securely side-by-side with personal email. This secure native client takes advantage of MobileNow's secure, native email policies including attachment encryption and data loss prevention, the ability to select specific attachment file types to encrypt, and the ability to restrict sharing of attachments with only approved business apps. For users with higher security requirements, MobileNow also provides secure, best-in-class third party email apps, or it can secure a 3rd party email app of the customer's choice. Secure third party e-mail clients incorporate all of MobileNow's MAM controls and app policies into the third-party email application experience, including encryption of all associated data, complete data control for file sharing, copy-and-paste and other editing functions, and controls for "jailbroken" devices, OS versions, blacklisted apps, geo-location, offline access, authentication and launch restriction. Last but not the least, MobileNow gives you the ability to block and revoke email usage for both secure native e-mail or secure third party email clients at any time.

AppSense DataNow

AppSense DataNow enables simple, secure access, sync and sharing of your enterprise files, no matter where they live. DataNow's unique approach does not require data migration or new storage. Since it leverages your existing IT storage and user authentication infrastructure, deployment and management is simple and straightforward.

- **Simple integration with existing storage**
  DataNow manages mobile file access through a virtual appliance that can be implemented in minutes. The DataNow appliance includes connectors to your existing storage locations, including user home directories, file shares, Microsoft SharePoint, WebDAV servers, and FTP servers. DataNow provides a single pane of glass for all of your existing files – no matter where they are stored – without the need to provision new storage or migrate data.
- **Simple anywhere data access experience that users will embrace**
  The DataNow broker works in concert with a collection of native applications for Windows, Mac, iOS, and Android, as well as an HTML5 web interface. DataNow lets you

give your users the same type of simple file sync and mobile access experience that draws them to services like Dropbox. The difference is that files are stored in your existing infrastructure, where they are both secure and compliant with your corporate and industry storage requirements. The result is a happy and productive user base without the security trade-offs.

- **Granular mobile data access policy controls**
  DataNow integrates simply with your existing Active Directory environment for user management and authentication. DataNow respects and enforces your existing file access controls and also adds an extensive set of mobile data access policies that address the unique challenges presented by mobile devices.
- **End-to-end security**
  DataNow lets you keep files secure without imposing VPN headaches on your users. All data is secured with 256-bit AES encryption as it is transferred between client devices and the DataNow appliance in your data center. Any files that users download to their tablet and smartphone devices are also encrypted on the device and can be wiped on-demand by an administrator.
- **No disruption to existing business processes**
  While DataNow simplifies mobile access to your existing files, users can also continue to access the same files through traditional methods such as mapped drives, SharePoint/WebDAV web interfaces, and FTP clients. You can enable new ways for users to be productive without disrupting existing business processes.
- **Simple and efficient team sharing**
  DataNow turns underutilized file servers into flexible team collaboration drives that users can work with productively from any PC, Mac, tablet, or smartphone. Users can get more done together without constantly transmitting sensitive files through e-mail or insecure cloud services.
- **Flexible, storage-agnostic approach**
  DataNow is designed to rapidly enable secure mobile access capabilities without imposing a proprietary storage model. It works with what you have while maintaining the flexibility to adopt new approaches like public cloud storage in the future – on your terms.

ARCHITECTURE

AppSense's EMM architecture is designed to balance ease and speed of deployment with the need to keep tight control over sensitive information. AppSense uses a hybrid SaaS/on-premises model as well as an on-premise approach. The MobileNow MDM, MAM, and secure e-mail functionality is delivered through either a 100% on-premises or a hybrid SaaS model that can provisioned for an organization instantly. Through the cloud-hosted console, administrators can perform functions such as OTA device provisioning, enterprise app store creation and management, device- and app-level policy definition and assignment, and many other administration and reporting functions. There is also a user view into the SaaS platform for self-service-based user on-boarding and management functions.

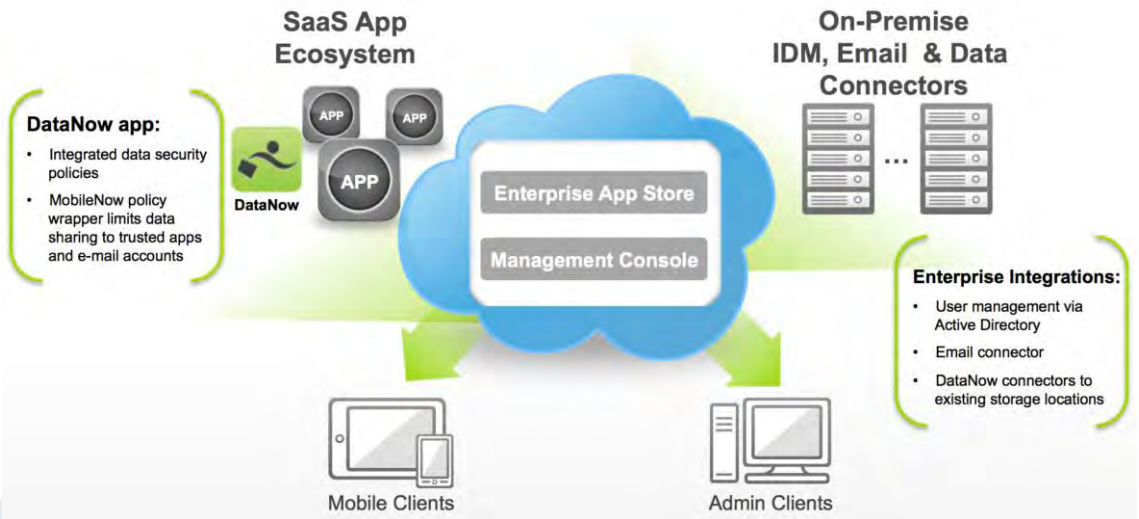
The AppSense approach utilizes a small and non-intrusive footprint on the customer premises to integrate seamlessly with existing enterprise systems such as Active Directory. DataNow mobile file access and sync functionality is provided through a virtual appliance that can be implemented easily in the DMZ or on the internal network depending upon the use case. (Pre-packaged virtual appliances are available for VMware, Hyper-V, and XenServer.) The DataNow

appliance includes connectors to existing storage locations such as file servers and works in concert with a collection of native applications for Windows, Mac, iOS, and Android, as well as an HTML5 web interface. In effect, DataNow gives users the same type of simple file sync and mobile access experience that draws them to consumer cloud storage services like Dropbox. The difference is that files are stored in the customer's existing infrastructure, where they are both secure and compliant with any corporate or industry storage requirements.

The fact that the DataNow architecture connects to existing storage locations with no need to migrate data is a major point of differentiation. Most alternative approaches require migration of data to vendor-provided cloud infrastructure, and even those vendors with on-premise storage options typically require the organization to migrate files from existing locations to a proprietary storage zone. In contrast, DataNow provides access to data in place. There is no need to provision new storage or migrate files. As a result, it is simpler to implement and does not disrupt any existing user workflows. Users can continue to access files through traditional methods such as mapped drives even as they gain new mobile access capabilities through DataNow.

The AppSense solution also uniquely addresses another important aspect of a sound EMM strategy: controlling data sharing between apps. Providing secure mobile access to files is an important first step, but the reality is the reason that users want to sync a file to a particular device is so they can made edits locally. Most EMM approaches either allow files to be copied into the insecure storage locations of untrusted apps or force the use of proprietary viewers and editors. With MobileNow, it is possible to wrap any third party application, as well as AppSense's own DataNow app with a policy layer that tightly controls data sharing. With this approach, users have the freedom to work productively with corporate files in their applications of choice while preventing the leakage of sensitive data to untrusted / unmanaged applications.

While AppSense MobileNow and DataNow each deliver significant stand-alone value, together they represent a comprehensive EMM approach.



LICENSING

AppSense MobileNow and DataNow are each available for purchase on a stand-alone basis, as well as combined as an enterprise mobility management (EMM) suite license.

AppSense's EMM suite is offered under annual per-user subscription licensing that includes software usage rights, ongoing updates, and support for a flat annual fee. Each licensed user may use MobileNow and DataNow on an unlimited number of devices.

AppSense MobileNow as a stand-alone solution is available on both per-user as well as per-device subscription licensing that includes software usage rights, ongoing updates, and support for a flat annual fee. Per user pricing is for unlimited number of devices per license.

AppSense DataNow as a stand-alone solution is available on per-user subscription licensing that includes software usage rights, ongoing updates, and support for a flat annual fee. Per user pricing is for unlimited number of devices per license.

8.4 CISCO MERAKI SYSTEMS MANAGER

INTRODUCTION

Cisco Meraki Systems manager is a freeware, cloud based (SaaS), solution to manage devices – mobile, Windows and MAC OS X devices. Systems Manager is an easy to use browser-based dashboard.

With Systems Manager, it is possible to centrally manage applications on iOS, Android, Mac OSX and Windows PC Devices. After installing the required software, any managed devices appear in the dashboard. Deployment from mobile applications to iOS, Android or Kindle is part of the solution. Systems Manager integrates with Google Play, Amazon Appstore for Android, Apple App Store and Apple's Volume Purchase Program.

Enforce policies across mobile devices administered by your organization. Protect devices and their data, control their usage with fine-grained passcode policies, and restrict access to the app store, gaming, and content. Systems Manager make it easy to define and deploy network settings like wireless connectivity, security settings and remote VPN access to all devices on your network at once.

Locate and track laptops and mobile devices anywhere in the world. Systems Manager provides built-in software inventory management, simplifying software license management even in multiplatform environments. Search and view details of all software and apps installed on your managed devices.

Bundle documents and files into a virtual backpack integrated into the Cisco Meraki dashboard. Seamlessly send content in the backpack over the air to one device or thousands. Use Systems Manager to effortlessly keep files and documents up-to-date with the latest versions on the server.

Device tags make content management and distribution easy. Prepare separate backpacks to be delivered to different classrooms, departments, or groups. Systems Manager automatically delivers selective content to the appropriate devices.

Fully Integrated with Meraki Networking Products

The Cisco Meraki cloud architecture provides the industry's only end-to-end solution which unifies WAN, LAN, wireless LAN, and mobile device management under a single pane of glass. Gain complete visibility and control from the top of the network, using MX Security Appliances, to the edge, with MS Switches and MR Wireless LAN, and even down to the client devices on the network, using Systems Manager

LICENSING

Cisco Meraki Systems Manager is free for unlimited amount of users and devices with basic email support. Phone support is available for Cisco Meraki customers who have purchased wireless LAN, switching or security appliances.

8.5 CITRIX XENMOBILE

INTRODUCTION

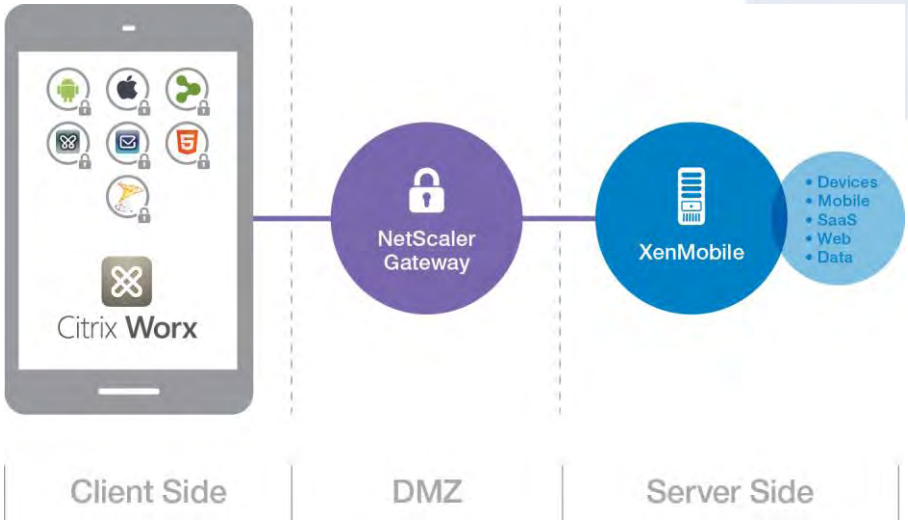
Citrix XenMobile is available in three editions:

- XenMobile Enterprise
- XenMobile App Edition
- XenMobile MDM Edition

With XenMobile, Citrix is able to offer a complete enterprise mobility management solution. XenMobile enables users to access their data, mobile, web/SaaS , Windows applications and desktops via Citrix Worx.

XenMobile provides identity-based provisioning and control for all apps, data and devices, including employee-owned devices. These capabilities enable IT to protect enterprise apps and data with policy-based controls, such as restriction of application access to authorized users, automatic account de-provisioning for terminated employees and remote wipe for data and apps stored on lost devices.

The Citrix mobile device management solution is included in both XenMobile MDM edition and XenMobile Enterprise. It delivers role-based management, configuration and security for both corporate and employee-owned devices. Upon user device enrollment, IT can provision policies and apps to devices automatically, blacklist or whitelist apps, detect and protect against jailbroken devices, and wipe or selectively wipe a device that is lost, stolen or out of compliance. Users can use any device they choose, while IT can ensure compliance of corporate assets and secure corporate content on the device.



The key features of XenMobile are:

Enterprise MDM

- Device management, Real-time Active Directory integration
- Policy configuration, Security and compliance
- Scalability and high availability, Ease of administration
- Provisioning and self-service enrollment
- Enterprise integration. Monitoring and support
- Device decommissioning

Unified app store

- Deliver mobile apps
- Deliver web/SaaS apps
- Deliver Windows apps (for XenDesktop/XenApp customers)
- Follow-me apps

Secure email, browser and data sharing apps

- Citrix WorxMail, Email encryption
- Citrix WorxWeb, Citrix ShareFile integration
- Microsoft SharePoint integration
- Citrix GoToAssist integration

Mobile app containers

- Mobile application management
- App wrapping

Identity management, single sign-on and scenario-based access control

- Leverage AD credentials, Instant app and data provisioning
- Single sign-on to apps and data, App requests
- Instant app and data de-provisioning

XenMobile editions

In addition to XenMobile Enterprise, Citrix offers XenMobile in two other editions: XenMobile MDM Edition and XenMobile App Edition. The MDM edition includes the enterprise MDM fea-

tures and the App Edition includes the Unified app store, productivity apps, mobile app containers and SSO features. The following table illustrates the differences:

	MDM Edition	App Edition	Enterprise Edition
Configure secure & provision mobile devices	•		•
One-click live chat & support	•	•	•
Access SharePoint & network drives	•	•	•
Secure mobile web browser	•	•	•
App-specific micro VPN		•	•
Secure mail, calander and contacts app		•	•
Enterprise-enable any mobile app		•	•
Seamless Windows app integration		•	•
Unified corporate app store		•	•
Multi-factor single sign-on		•	•
Secure document sharing, sync & editing			•
Both cloud & on-premises data storage options			•

ARCHITECTURE

The main component in XenMobile is the App Controller. The App Controller aggregate, control, and deliver Web, mobile, SaaS apps, and ShareFile documents to any user on any device. App Controller empowers users with a single point of access and self-service for the apps from any device. It also provides contextual controls and automated provisioning of user accounts for supported applications. Users can connect with self-service to access their applications and documents.

The other key component is XenMobile Device Manager. The Device manager allows IT to manage mobile devices, set mobile policies and compliance rules, gain visibility to the mobile network, provide control over mobile apps and data, and shield the corporate network from mobile threats. With a “one-click” dashboard, simple administrative console, and real-time integration with Microsoft Active Directory and other enterprise infrastructure like PKI and Security Information and Event Management (SIEM) systems, XenMobile Device Manager simplifies the management of mobile devices.

Other components are:

- NetScaler Gateway is a secure (application) access solution that provides administrators granular application-level policy and action controls to secure access to applications and data while allowing users to work from anywhere.
- The MDX Toolkit includes a software application that you can install on Mac OS X Version 10.7 devices. The tool converts unsigned iOS or Android mobile apps into signed Citrix Mobile Application (.cma) or MDX files. In the process of this conversion, Citrix embeds a policy framework and default set of policies that allow you to configure, securely distribute, and manage each prepared application by using App Controller.
- Citrix Worx is client software installed on the user device that allows users to access their apps and data through App Controller.

XenMobile also works with Citrix StoreFront that integrates with your existing Citrix XenApp and Citrix XenDesktop deployment enabling you to deliver Windows applications and virtual desktops to any device through a unified self-service storefront. StoreFront works with XenMobile extending the unified applications store beyond Windows applications and virtual desktops to Web, SaaS, mobile applications, and ShareFile.

LICENSING

XenMobile offers a per-user and per-device licensing model. Per-user licensing is based on the total number of users that access the software, regardless of the number of devices they are using, whereas the per-device licensing is based on the total number of devices that access the software. XenMobile is available with a perpetual license or an annual license.

XenMobile MDM and XenMobile App Edition can be bought as a separate products. XenMobile MDM will bring Secure, simple to use Mobile Device Management for SMB & Enterprise, and is also available as a Cloud service. XenMobile App Edition will bring mobile application management for native mobile app delivery and secure email and browser apps to users on any device.

8.6 GOOD FOR ENTERPRISE

With Good for Enterprise you can:

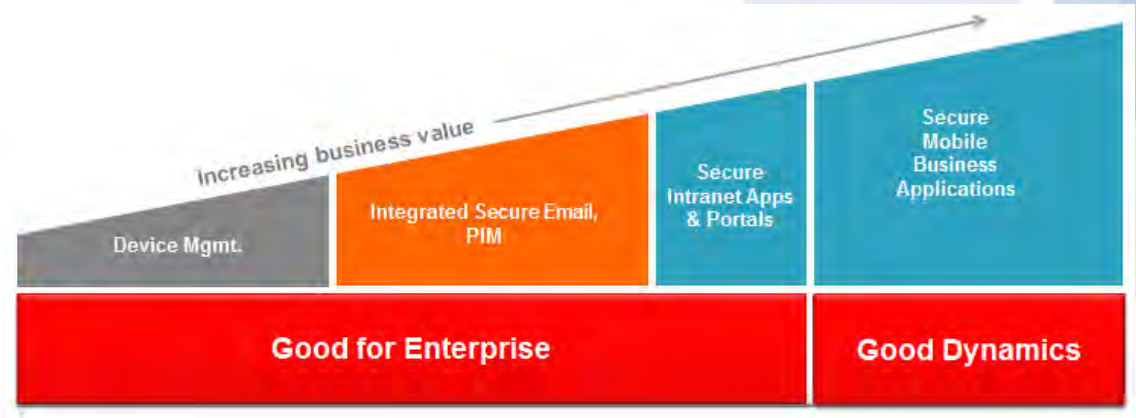
- Manage and control almost all mobiles within the organization
- Secure mobile email and collaborate with employees
- Gives you securely access to calendars, contacts, tasks, etc
- Provide two-factor authentication and S/MIME email signing and encryption
- Secure Browser which gives you access to your corporate intranet sites, applications and data (which might be SharePoint) without the need for a VPN
- securely containerize and control mobile apps and data

With Good Dynamics you can:

- Use instant message (IM) and presence on mobiles (Good Connect)
- Access, sync and share files from Sharepoint and other file servers behind the corporate firewall (Good Share).
- Strong two-factor authentication and S/MIME email signing and encryption to Good for enterprise to secure mail access (Good Vault)
- Provides enterprise app store capabilities where customers can easily provide access to applications that they want enabled within the company (App Central)
- Deliver secure mobile apps to the field, and securing the application data with end-to-end security (Good Dynamics Marketplace)

INTRODUCTION

Good Technology is based in Sunnyvale, California. Good for Enterprise (GFE) is a mobility suite that supports mobile collaboration, with strong support for security and management. The following suites are part of Good's product portfolio;



- Good for Enterprises, for MDM, local data store, secure (intranet) browser and secure wireless email and PIM.
- Good Dynamics, for developing (SDK), securing and deploying containerized applications.
- Good Boxtone, for Mobile Lifecycle Management, Mobile Service Management, Mobile Application Management and Mobile Application Analytics.

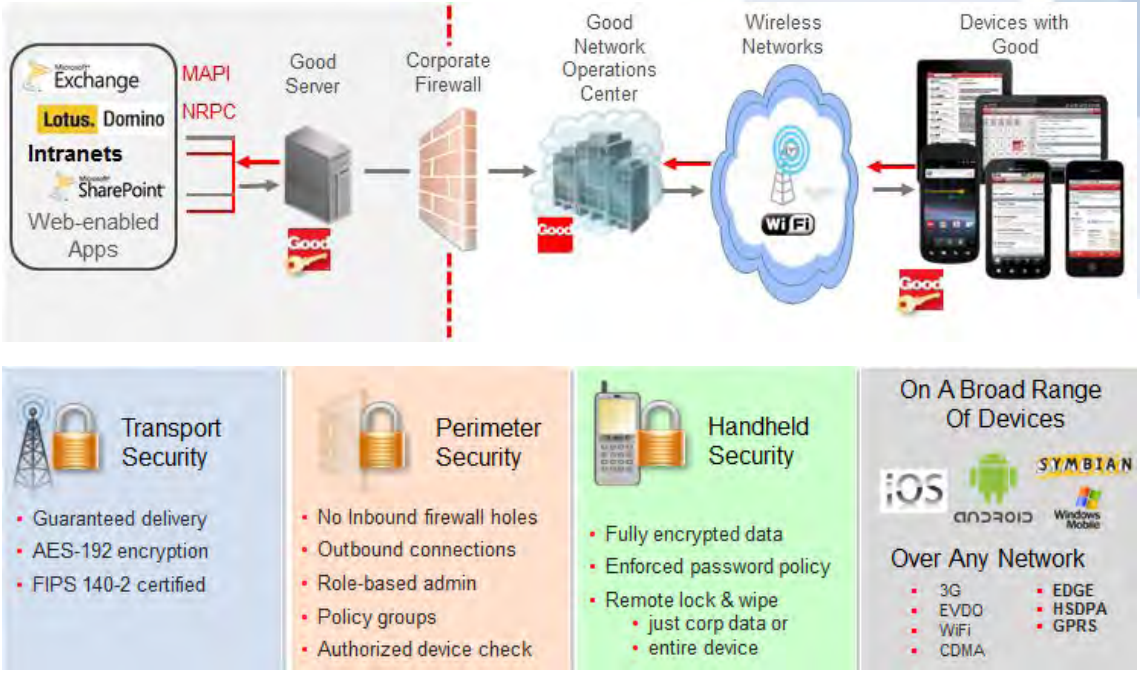
The management and security capabilities of Good for Enterprise require the installation of the Good Mobile Messaging client on devices. This client ensures secure access to corporate intranet sites, applications and data that are inside the company firewall without requiring a VPN infrastructure. Good Vault adds support for Common Access Card integration and security features, such as S/MIME. (S/MIME is also supported within GFE for email signing and email encryption).

Good for Enterprise is recommended for companies that want strong security support for their mobile devices, and for those customers concerned about the legal liabilities of intermixed business and consumer information.

With Good Dynamics companies can utilize the many 3rd party Good Dynamics apps and create and deploy (custom made) apps to a secure container on the mobile device. With App-Kinetics, a technique patented by Good, data can be securely transported between GFE and Good Dynamics enabled Apps (or between Good Dynamics enabled Apps) and policies can be configured to allow data-sharing between the secure containers seamlessly through single Sign-on. A special developed Good SDK allows companies to create their own “Good” apps and publish them internally or through the “appstore” after integrity verification by Veracode.

ARCHITECTURE

The architecture of Good consists of two mayor components; On-premises Good servers and the Network Operations Center (NOC) which is a datacenter hosted by Good. Together they establish the end-to-end security solution where the technology of Good is based on.



The minimal configuration of the on-premises part consist of a Good Mobile Messaging server (GMM) and a Good Mobile Control server (GMC). Both applications can be installed on one server.

Good Mobile Manager (GMM) is responsible for managing the personally owned and corporate issued smartphones and tablets.

The Good Mobile Control Console (GMC) provides the primary Web Based console that can be used to; add users/devices to the system, Configure policies that manage the device and monitor the device after they are set up.

The GMM server will only create an outbound encrypted connection with the NOC. Because no inbound connections will be established from the internet, a server in the DMZ is not needed or recommended. Because the initial session setup to the NOC from the GMM server is outbound only, it acts as a regular proxy client in the network. The mobiles that should be managed can be provisioned with an (over-the-air) OTA policy. If a mailbox is provisioned, the user receives a notification e-mail with instructions and pincode (this can also be disabled and the information can be supplied to the end user via a different method if needed), allowing the user to install the mobile app from the “appstore” and establishing an AES 256 bits encryption through the NOC with the GMM on-premises server. The data on the mobile and encrypted connection between the mobile and the GMM is certified with the highest cryptographic modules to protect data-at-rest and data-in-transit (FIPS 140-2). Because the encryption keys are generated on the mobile device and on the GMM server, the NOC has no keys of what so ever to decrypt or inspect the content of the traffic. This ensures that hackers cannot decrypt the traffic. The NOC serves as a connection point for the mobiles and a pass through datacenter.

Good for Enterprise

Good for Enterprise is a secure mobile email and collaboration suite that increases employee productivity and satisfaction without compromising security. It delivers an integrated, intuitive user experience that allows employees to access corporate email, documents, contacts, calendar, tasks and intranet from any device. The Good app on the mobile looks the same as the native apps but has more functionality. Good for Enterprise protects corporate data in-use and at-rest on the device through a secure (encrypted) container that separates business data from employee's personal information. Through different policies and settings it is possible to implement company policies regarding managed and unmanaged devices and prevent data-loss with a stolen or lost mobile device.

Good Dynamics

Good Dynamics suite consists of the following components:

Good Vault, extends strong two-factor authentication and S/MIME email signing and encryption to Good for enterprise to secure mail access, ensure message privacy and integrity, and enhance data protection. User keys and credentials can be stored on smartcards and microSDs, so that the form factor of the mobile, or user experience will not be compromised.

- For the C-Suite:
  - Protect corporate data with strong two-factor authentication (PIN, Secure Element card)
  - Prevent data loss with S/MIME* encryption with the credentials stored in a Secure Element
  - Comply with the highest standards and regulations
  - Comply with HSPD-1, FIPS, FFIEC, PCI-DSS, HITEC, HIPAA and more
- For IT Managers:
  - Extend the same email and data security on desktops and laptops to smartphones
  - Leverage card-based identity management without heavy or clumsy standalone readers
  - Support Secure Elements on PIV/CAC and microSD cards
  - Integrate into existing PKI environments to maximize your legacy investments
  - Meet the requirements of Security and Information Assurance for mobile IAM
- For the Mobile-Workers:
  - Collaborate on mobile devices securely to stay productive on-the-go
  - Enjoy unmatched convenience, usability, and portability
  - Use a card reader that maintains the sleek phone design

Good Connect is an enterprise instant message (IM) and presence app that can be used for communication and collaboration. It extends corporate IM platforms (like Lync, OCS or Lotus Sametime) to mobile devices without requiring VPN, firewall holes or servers in the DMZ.

- Key Employee Features
  - Keep personal contacts and IMs private
  - View colleagues' real-time presence and availability
  - Select the best way to communicate: IM, email or phone
  - Receive message alerts, even when the app is in the background
  - Swipe contacts for quick actions like blocking or deleting
  - Search corporate directory for contacts

- Manage multiple chats in conversation view
- Search conversation history, even in offline or airplane modes

- **Key IT Features**
  - Protect corporate data in motion and at rest with military-grade encryption
  - Secure the corporate network by not requiring firewall holes or servers in the DMZ
  - Configure granular security policies (such as strong password requirements)
  - Prevent data leakage by disabling cut/copy/paste and separating work and personal contacts
  - Lock or wipe corporate data remotely while preserving personal information

Good Share Provides fast, easy access to Sharepoint and corporate file shares, all with secure transport and storage to protect your corporate data and resources. Good Share enables workers to access, sync and share corporate documents instantly with no VPN, no firewall re-configurations, and no need for extra file stores.

- Key features:
  - Ensure data security with separate containers for corporate and personal information
  - Protect data in transit with NOC-based, AES-encrypted transport to and from devices
  - Manage document actions through granular policy controls
  - Wipe corporate data remotely without impacting personal data
  - Enhance mobile productivity with a secure access to email, document editors, and more

AppCentral provides enterprise app store capabilities where customers can easily provide access to applications that they want enabled within the company. These can be: 3rd party apps, Good Technology Apps or their own apps. This provides the end user with a familiar interface to browse for, and install corporate approved applications with a Apple App Store/Google Playstore interface. Users can also rate applications and give feedback on applications through this app store.

Good Dynamics Marketplace is a comprehensive solution for enterprises tasked with quickly delivering secure (custom made) mobile apps to the field. It lets developers get their apps out the door fast- but with a layer of security that is (according to Good) unmatched in the industry. It addresses challenges of accessing corporate data through the apps and securing the data with an end-to-end encryption. A deployed app serves as a local encrypted container to ensure that company data is secured and to prevent data loss through copying information to consumer applications like Dropbox or Skydrive.
Key features:

- Containerize any app. quickly embed encryption and policy controls into your custom apps, even when source code is unavailable. (Through AppWrapping)
- Secure app-to-app communication. Use patent-pending inter-app communication technology (App-Kinetics) to automatically secure document transfer between Good Dynamics-enabled apps (e.g. open in) as well as Good for Enterprise.
- Enable policy controls. Empower IT to enforce app-level security controls for jailbreak and root detection, password, lock/wipe, compliance, app-specific custom policies and Data Loss prevention (DLP).

- Change policy dynamically. Allow IT to modify policy over the air at any time without requiring an app update.
- Cross platform security. Permit IT to control apps for iPhones, iPads, Android phones, tablets, and even HTML5 apps.
- Prevent security exploits. Block rogue app and malware access via jailbreak detection and app/device authentication validation.
- Secure infrastructure. Automatically encrypt app data in motion and provide app-level authentication outside the firewall.
- Ensure fault tolerance. Prevent loss of operations and improve performance with high-availability and disaster recovery (HA/DR) support.
- Extensive app library. Off-the-shelf apps to address any business need, all built on the Good Dynamics mobile app security platform.

LICENSING

Good for Enterprise is perpetual licensed per server and per device (CAL). Support is a (multi) year fee. Good Dynamics is based on yearly subscription (support included) per device and per app. Server license is included. Third party apps licensing vary per ISV.

8.7 MAAS360 BY FIBERLINK

MaaS360 is a comprehensive enterprise mobility management platform that spans across users, devices, documents, apps, the web, and usage expenses. The MaaS360 product line is as follows:

- MaaS360 Mobile Device Management
- MaaS360 Mobile Application Management
- MaaS360 Application Security
- MaaS360 Mobile Content Management
- MaaS360 Secure Mail
- MaaS360 Secure Browser
- MaaS360 Enterprise Gateway
- MaaS360 Mobile Expense Management
- MaaS360 Laptop Management

INTRODUCTION

Businesses use MaaS360 to provide their employees with secure access to corporate resources and information from personal and corporate mobile devices, without compromising the user experience, data security or privacy. MaaS360 delivers maximum flexibility for bring your own device (BYOD) with a dual persona approach, multi-platform support, self-service enrollment, customized over-the-air configuration, automated policy enforcement, and secure distribution of apps and documents. MaaS360 provides a range of product modules and bundles to enable customers to effectively meet their mobility requirements.

More Than Just Mobile Device Management

MaaS360 provides complete end-to-end management and security for managing mobile devices. This includes all the necessary features such as over-the-air enrollment, configuration, security policy management, and remote actions.

More advanced MDM features include:

- Automated Compliance Monitoring and Threat Mitigation – Monitoring and rules-based actions trigger on-device compliance related to the current policy, and compliance rules (OS version, encryption support, application compliance, jailbroken/rooted status, enrollment status, SIM change). Events are logged, and compliance rules can enforce automated functions (notify, restrict device, wipe) when a non-compliance is detected.
- Location-Based Policies – Dynamic policy assignment based on a geo-physical location or network connection. The policy in effect can change on an automated location check in/out. Geo-fencing rules take action (alert, change policy, wipe) when a device enters or leaves a specified location.
- BYOD Privacy Settings – Disable the automatic collection of personal information (app information, location information and network information) on a single device, all devices, or specific device groups.
- Enterprise Integration – MaaS360 Cloud Extender seamlessly integrates with enterprise systems such as Microsoft Exchange, Microsoft Office 365, Gmail, Active Directory, LDAP, Lotus Traveler and Certificate Authorities. A robust set of APIs are available to integrate with other systems such as NAC, SIEM, TEM, and other 3rd-party IT infrastructure systems.

Managing and Securing Mobile Apps

MaaS360 provides the ability to remotely distribute, update, and manage private, public, and purchased apps across mobile devices. MaaS360 App Catalog is an on-device enterprise app store for users to easily view available apps, install them, and be alerted to updates:

- Selectively remove managed apps
- Blacklist and whitelist apps
- Track app inventory, versions and compliance
- Supports volume purchasing
- View detailed reports of app compliance events and remediation actions
- Optional MaaS360 App Cloud for scalable hosting & distribution

MaaS360 can containerize enterprise and third party apps (via wrapping or SDK) with app-level policy enforcement to protect against data leaks, require authentication, restrict cut/copy/paste, prevent data backups to online services, send policy violation alerts, remove apps as part of device/corporate wipes, plus require full compliance prior to app launch/execution. This includes Application Quarantine features, where app execution requires the following:

1. The device is compliant with the current policy
2. The user is authorized
3. The application has not been tampered with
4. The application is not on the application blacklist
5. The application has not been flagged as malware by MaaS360's application reputation module

Distributing Corporate Documents

MaaS360 mobile content management is a set of content management, security, and productivity tools with the ability to centrally control mobile documents, access controls, distributions and policies. It includes the MaaS360 Doc Catalog, an on-device password-protected container that provides a secure and simple way for users to access, view, and share documents.

Documents managed through MaaS360 can be edited, managed with version controls, audited, and expired based on time.

Data Loss Prevention (DLP) policy options include requiring user-based authentication, restricting copy/paste functionality and blocking documents from being opened or shared in other applications. MaaS360 integrates with corporate document stores such as SharePoint, files shares, and network drives. The optional MaaS360 Document Cloud is available for scalable hosting & distribution.

Dual Persona Options for Securing Data

MaaS360 Secure Productivity Suite is a separate and secure office productivity app for users to access and manage email, calendar, and contacts. It includes the ability to control emails and attachments to prevent data leaks by restricting features to forward or move content to other applications, enforcing authentication, restricting copy/ cut/paste, and locking down documents:

- Protects email text and attachments by preventing them from being shared with other applications
- Policy control of attachments, with the ability to wipe them outside of the email application
- Does NOT require inline email infrastructure (vs. traditional secure mail vendors) and provides end-to-end control
- Mail does not “flow” through Fiberlink data centers.
- Passcode protection with configurable timeouts, offline compliance checks before allowing email access, FIPS 140-2 compliant AES-256 encryption
- Superior email security over "attachment stripping"
- Supports both iOS and Android
- Supports corporate- and third-party-wrapped applications

ARCHITECTURE

The MaaS360 platform is an open, extensible, multi-tenant, change-ready platform that is offered to IT administrators as a Software as a Service application for securely managing mobility in a hosted, client / server architecture.

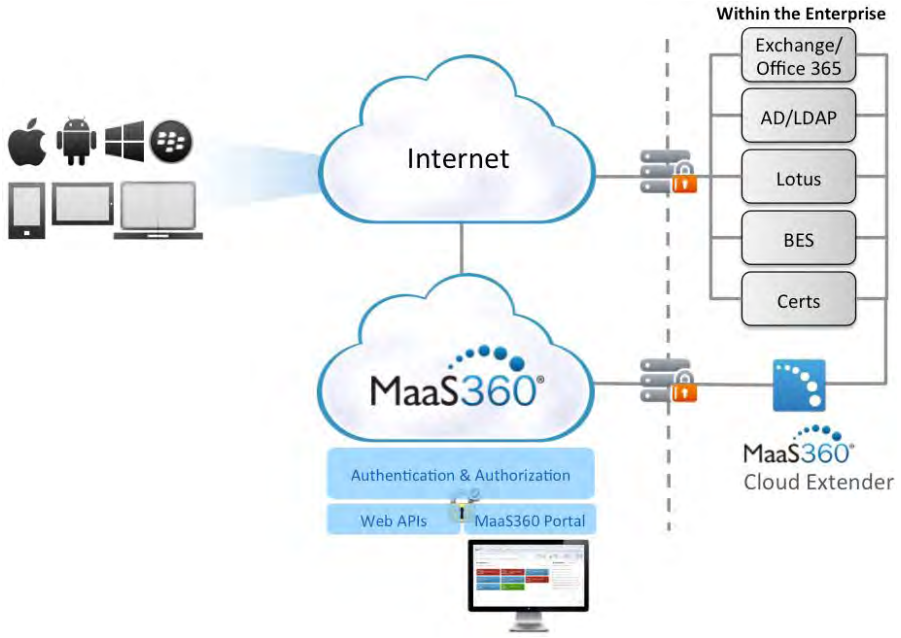
It offers IT professionals an Enterprise Mobility Management solution that connects, controls and protects all enterprise mobile devices and data.

Through a single management console the administrator can initiate device enrollment, configure compliance rules and alerts, set up and assign policies, view interactive dashboards and reports, and conduct advanced searches. The MaaS360 architecture also provides robust application programming interfaces (APIs).

The MaaS360 Cloud Extender provides the ability to securely integrate with enterprise systems including Exchange ActiveSync (EAS), Active Directory and LDAP, Lotus Traveler, BlackBerry Enterprise Server, and Certificate Authorities. The MaaS360 Cloud Extender is patented technology that provides valuable, plug and play integration between important systems within your infrastructure and the MaaS360 platform in a non-intrusive and secure manner.

It supports the following integration features:

- Exchange ActiveSync and Traveler – The Cloud Extender provides instant visibility into all of your existing devices connected to the mail system, and enables auto-quarantine functionality to prevent any new devices connecting without authorization.
- Active Directory and LDAP – The Cloud Extender facilitates AD/LDAP authentication for self-service enrollment and grouping for the assignment and distribution of policies, apps and docs as well as administrative role-based access.
- Certificate Authority – The Cloud Extender facilitates the automatic provisioning of digital certificates for wireless, VPN, and email profiles.
- BlackBerry Enterprise Server – The Cloud Extender uses the BlackBerry Enterprise Server (BES) APIs to provide complete visibility and control of BlackBerry devices (BlackBerry 10 device support in development).
- Mobile Enterprise Gateway – The Cloud Extender can be configured to provide secure mobile access to behind-the-firewall information resources and a more efficient and targeted approach than traditional VPNs.



LICENSING

MaaS360 is offered as a subscription service that includes set up, upgrades, maintenance, and 24x7 customer support. Subscriptions are priced based on the functionality required and the number of devices or users licensed. Per-user-based pricing provides for an unlimited number of devices for individual users (smartphone, tablet, laptop).

8.8 MICROSOFT EXCHANGE ACTIVESYNC

Microsoft Exchange ActiveSync is part of the Microsoft Exchange platform (including Office 365). Since Microsoft Exchange is used a lot in enterprises, it's good to know that with Microsoft Exchange ActiveSync some MDM features are available.

INTRODUCTION

Microsoft Exchange ActiveSync is the protocol used by mobile devices to communicate with the Microsoft Exchange Server. This is primarely designed and used for synchronization of email, contacts and calendering tasks from the server to the device. However, Mobile Device Management features are also built-in to provide some policy controls.

These Mobile Device Management features are not as complete as a true MDM solution but at least enable you to:

- Limit reply/forward of corporate email
- Block specific devices
- Remote wipe
- Required password and password length
- Number of failed attempts.

Microsoft Exchange ActiveSync provides the simplest protection for your mobile workforce. If your on Exchange Server or Office 365 and you have no additional MDM solution in place, using Microsoft Exchange ActiveSync services could be the "better-then-nothing" solution.

8.9 MICROSOFT WINDOWS INTUNE

With Windows Intune you can:

- Publish applications in a company portal
- Manage updates and proactively monitor PCs
- Protect PCs from malware and set security policies
- Provide remote assistance (no support on Windows 8 yet)
- Inventory hardware and software
- Upgrade to Windows 7 Enterprise or run select prior Windows releases

INTRODUCTION

Windows Intune is a Microsoft cloud-based (SaaS) management solution which was introduced in July 2011. When it debuted in 2011, it was a PC-management and security service. With the release of Intune 2.0 (new feature in software distribution) and 3.0 (device management via Exchange ActiveSync, supporting iOS and Android) the product became more cloud-aware. In January 2013 release 4.0 (also known as Wave D) was introduced, which added support for the latest mobile devices. This includes Windows 8, Windows RT and Windows Phone 8.

Intune can be used for PC-management and mobiles devices which are not Active Directory domain joined. Because of Exchange ActiveSync (EAS) limitations, Microsoft is making a transition from EAS to Mobile Device Management (MDM). Therefore, an agent needs to be installed on the device, which is more powerful. Microsoft platforms (including new mobile platforms) and Apple's iOS has support for this agent, but Android is still EAS-based in this release.

It is possible that in the next release (Wave E) Android will be agent-based also, which offers new features. That way the same functionality can be offered on Windows, iOS and Android. At the meantime both EAS and MDM are used to support mobile devices.

The following table lists the supported operating systems for each of these device types:

Device	Operating System	Management
Microsoft Surface	Windows RT	Direct
Windows Phone 8	WP 8.0	Direct
Windows Phone 7	WP 7.x	EAS
iPad, iPhone, iPod Touch	iOS 4.0 or later	Direct
Android-based devices	Android 2.1 or later	EAS
Microsoft Surface Pro	Windows 8	Direct
PC devices	Windows XP SP3, Vista, 7, 8	Direct

With a new release every 6 months Windows Intune offers support for the latest mobile devices. With every release there may be new and better features enclosed also. Microsoft brings many features for PC-management and mobiles devices and offers a truly cloud-based management solution with Intune.

ARCHITECTURE

Devices in Windows Intune can be managed with a web portal in the cloud or within System Center 2012 Configuration Manager (SCCM). Both solutions have their own benefits. When creating an account on Intune, an account portal, admin console and company portal become active. When combine Windows Intune and SCCM, management is done completely in SCCM. To combine both products, SCCM 2012 with Service Pack 1 must be in place. EAS support is available for both solutions with an Exchange connector. With a SCCM connector in place there is support for up to 100.000 computers.

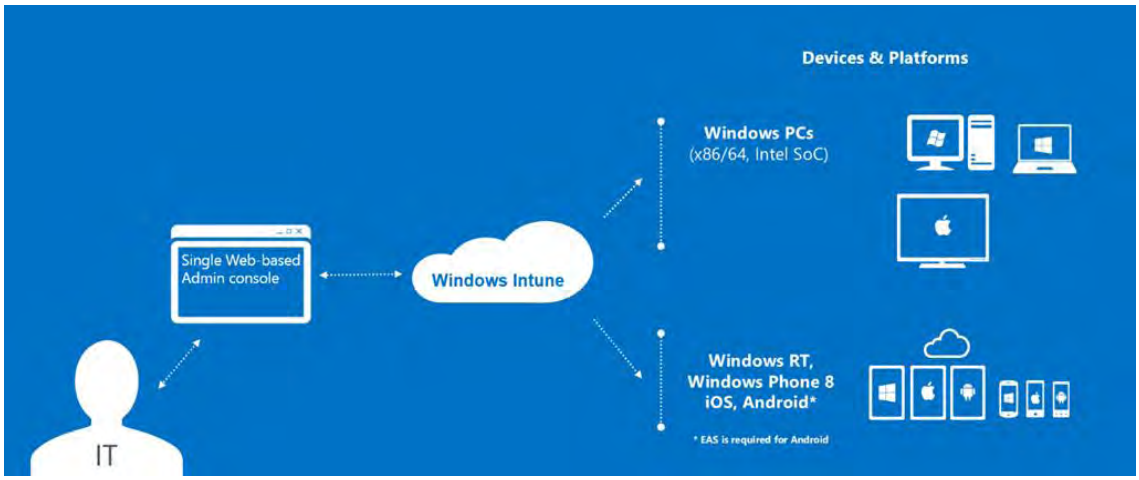


Figure 1: Windows Intune

Figure 2: Windows Intune with System Center Configuration Manager

The following can be found in Windows Intune:

Account portal

The account portal lets you manage your Intune subscription and specify the users who can access Intune. From the account portal, you can perform tasks such as manually adding user accounts and security groups, setting up and managing service settings, checking service status, and accessing online Help. You can also access the administrator console and the company portal from here. Users can access the account portal to change their password.

Admin console

The admin console is used for doing daily management. In this console (which is based on Microsoft Silverlight) user/device groups, software updates, endpoint protection, software packages, and policies are managed. The console can be started from anywhere, anyplace, as long Silverlight 3.0 is installed. No need to install a fixed console, just open it from a device and start managing. The only thing needed is an administrator account for Intune.

The following can be found in the admin console:

- **System Overview**: Dashboard with information about endpoint protection, software updates and agent health. Also alerts by type are displayed.
- **Groups**: Create and manage user/device groups and have a look how many PCs and mobile devices are managed. Management can be done per group or device.
- **Updates**: Updates, which is WSUS in the cloud, is used to configure and approve software updates. It is also possible to create automatic deployment rules.
- **Endpoint Protection**: Anti-virus management with a malware dashboard and the possibility to configure agent settings.
- **Alerts**: One overview with all kind of alerts. Configure alert type settings and notification rules to receive alert messages by e-mail.
- **Software**: Add software packages and manage deployments. Software packages can be deployed to the company portal.
- **Licenses**: Add and manage license agreement information for Microsoft or non-Microsoft software that was purchased by other means.

- **Policy**: Deploy and manage settings for endpoint protection, software updates, windows firewall and end-user experience. Also control security on mobile devices.
- **Reports**: Run reports for software, hardware and software license information. Reports can be saved for later usage also.
- **Administration**: View details about your Intune account and perform daily tasks on updates, alerts and notifications, client software, storage use and MDM.

When integrating Windows Intune in SCCM, daily management is done in SCCM instead of Intune. No need to open the admin console for management anymore.

Company portal

The company portal is used to enroll/manage devices and make applications available to end users. All applications deployed to users, which are optional, will be automatically displayed in this app store. Included are applications for PCs and mobile devices, based on Windows, iOS or Android platforms. Applications can be added as a file or with a link in the vendor's app store. That way it's not needed to have all application files available.

Applications can be created as a software-package or an external link. The following platforms are supported: Windows PCs, Android, iOS, Windows Phone, and Windows 8 app package. The following external links are supported: Windows Store, Windows Phone Store, Apple App Store, or Google Play.

Applications can be deployed by user (optional installation) or by device (mandatory installation). Only optional installations will be displayed in the company portal. Mandatory installations will be installed on the user's device automatically.

LICENSING

Licensing is done on a per user basis, for up to five devices per managed user. This release of Windows Intune adds new licensing options for managed users with multiple devices, rather than focusing on a per device basis. This new approach can provide more flexibility to organizations that plan to implement a "bring your own device" strategy.

The following licensing options are available:

- **Windows Intune**: Basic licensing for users with up to five devices. It also includes use rights to SCCM for integration with Windows Intune.
- **Windows Intune with Windows Software Assurance**: Same as basic licensing, with the difference that SA can be used on one of five devices. It is a good option for organizations that need to upgrade PCs to Windows 8 Enterprise.
- **Windows Intune Add-on for SCCM**: For organizations with an existing System Center volume licensing agreement. Manage both existing SCCM managed devices and new mobile devices using the SCCM management console.

8.10 MOBILEIRON

INTRODUCTION

MobileIron was founded in 2007 and headquartered in Mountain View, California. In 2009 MobileIron launched MobileIron V1, the first version of MobileIron's mobile management so-

lution. MobileIron was purpose-built to secure and manage mobile apps, docs, and devices. Mobile is how people work in the post-PC era, but mobile introduces risk, cost, and usability challenges that traditional IT strategies cannot address. MobileIron enables people to get their work done by:

- Protecting data
- Mobilizing apps and docs
- Preserving user experience and privacy
- Supporting a constantly shifting mobile OS and device landscape
- Deploying at massive scale to end users across a global organization

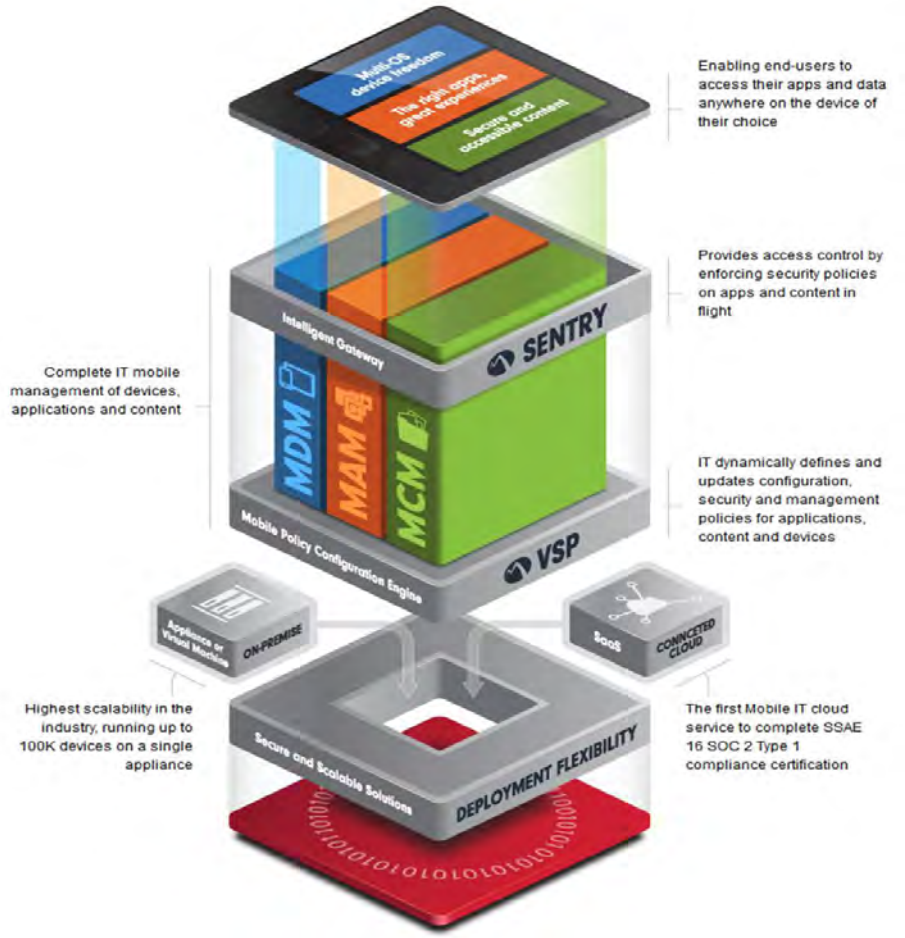
ARCHITECTURE

The MobileIron architecture has three main components:

- **End-user services** to secure and manage email, apps, docs, and web. These services are directly accessed by end users from their devices through the MobileIron client. MobileIron provides delivery, configuration, and data-at-rest protection. Protection for these services. The client also does ongoing posture and compliance checking.
    - Apps@Work is the enterprise app store
    - Docs@Work is the mobile content management offering
    - Web@Work is the mobile secure browser offering
    - AppConnect is the client-side containerization capability (SDK and wrapper) for securing data-at-rest
- **Intelligent gateway** to secure and manage access to the enterprise. This gateway securely tunnels traffic from the end-user services to back-end enterprise resources like Exchange, app and web servers, and SharePoint.
    - This gateway is called MobileIron Sentry and it protects data-in-motion for email, apps, docs, and web**.** The MobileIron Sentry can be installed as either a physical or virtual appliance**.**
    - AppTunnel is the implementation of Sentry for secure apps tunneling
- **Policy and configuration engine** to ensure mobile apps, docs, and devices can be managed end-to-end at global scale**.**
    - The engine is called the MobileIron VSP for on-premises deployents. The MobileIron VSP can be installed as either a physical or virtual appliance**.**
    - The engine is called the MobileIron Connected Cloud for cloud deployments.

The MobileIron solution can be deployed in two ways:

- Public cloud: MobileIron Connected Cloud is the multi-tenant cloud service hosted by MobileIron.
- Private cloud: The MobileIron VSP (Virtual Smartphone Platform) is deployed on-premises. The MobileIron VSP and MobileIron Sentry can each be deployed as:
    - On-premises virtual appliance: hardened VMware or Hyper-V Linux appliance
    - On-premises physical appliance: hardened physical Linux appliance



App Delivery Network

The MobileIron App Delivery Network offloads app provisioning to a highly secure external network that provides reliable app delivery without load or latency. The App Delivery Network reduces the load on the corporate network and is seamlessly integrated with the MobileIron platform. Once the App Delivery Network is enabled, it manages app provisioning without changing the end user's experience; end users download and update their apps as usual. MobileIron provides an one-step integration with the MobileIron VSP, no firewall, DNS, or LDAP changes are needed.

LICENSING

The core product licensing of MobileIron is per device. Customers can choose a perpetual license or per month subscription licensing model. Per user licensing is also an option with 20% cost raise. Support is included when choosing an subscription license, with the perpetual licence support is bought at an extra annual fee.

The MobileIron on-premises deployment can be licensed with perpetual and subscription licenses. And the MobileIron Connected Cloud is only available as a subscription license. MobileIron also has several add-on products that are sold through bundles.

8.11 SYMANTEC MOBILE MANAGEMENT SUITE

INTRODUCTION

Mobility without Vulnerability

Technology is on the move. The mobile devices that employees have mastered on their own personal time are becoming timesaving tools for enterprises. With the growing potential for any-time, any-place productivity comes the expanded risk of lost data, breached confidentiality—and even broken laws. Enterprises today are looking to provide a seamless experience for interacting with both enterprise data and personal information, compromising neither productivity nor privacy. Enterprises require a mobile productivity solution that enforces IT controls without imposing user obstacles, independent of device ownership. Symantec™ Mobile Management Suite serves both masters, the professional and the personal, enabling a seamless user experience that encompasses multiple aspects of mobility across multiple deployment models: enterprise-owned, employee-owned (BYOD), or a hybrid mixture of the two. The suite replaces conflict with co-existence of the professional and the personal activities through one solution addressing the five essential pillars for mobility: User and App Access, App and Data Protection, Device Management, Threat Protection, and Secure File Sharing. The Mobile Management Suite enables mobile workforce productivity without compromising protection.

Overview: Symantec Mobile Management Suite

Mobile Management Suite is a comprehensive mobile solution providing the capabilities needed for enterprises to enable the productivity of their mobile workforce without sacrificing protection. The suite enables seamless and secure coexistence of personal and professional activities. With innovative application management, scalable device management, and trusted threat protection Mobile Management Suite enables the professional and the personal coexistence by providing the following core capabilities:

- **App Wrapping**
  Corporate apps are containerized using a unique technology that does not require source code changes and enables clear separation of corporate and personal data on the device. Mobile Management Suite can wrap a layer of security and policy management around any mobile app, without any source code changes or SDK embedding. App developers do not have to be security experts to deliver secure apps for the enterprise. App protection policies include secure app connectivity, user authentication, data encryption, writing data to local storage, document sharing, copy/paste, and offline access. The suite provides secure app connectivity by providing a per app wrap policy that enforces a secure SSL connection and blocks apps from going to unauthorized sites.
- **App Distribution**
  The suite provides advanced app management and protection capabilities for easy distribution of mobile apps and content. The suite allows distribution of apps to employees and other authorized users with appropriate corporate security and data protection. Apps and data can be revoked quickly and securely when employees leave or devices are no longer active.
- **Corporate E-mail Access**
  The suite enforces access control policies for mobile email and enables advanced allow/restrict rules based on groups, device compliance, and device attributes. Features include automatic configuration for native and third-party email clients (such as Nitrodesk TouchDown) that connect to mail servers like Microsoft® Exchange, Office 365, Gmail, and Lotus Notes.
- **Authentication and Single Sign-on**
  The suite provides a simple and secure user experience via strong authentication methods. The suite supports authentication requirements on email, Wi-Fi and VPN, and integrates with Symantec™ Managed PKI Service and Microsoft Certificate Authorities. The suite provides integrated single sign-on functionality across in-house and third-party apps, leveraging popular authentication methods including LDAP, SAML and SiteMinder®. In addition, the suite extends single sign-on to cloud apps through integration with the Symantec O3 web gateway.
- **Device Management**
  The suite provides comprehensive mobile device management capabilities providing visibility and control over smartphones and tablets. The suite enables devices to access key corporate assets, such as email, calendar, critical mobile applications, documents, and media content. The suite helps ensure corporate compliance by enabling advanced security settings on devices. All policy options including passwords, remote wipe, and resource and app restrictions can be targeted to a specific user/device/OS/group.

- **Compliance and Remediation**
  The suite enables administrators to allow only compliant devices. For mobile device management, define compliance using device status (jailbreak, encryption), user status (group membership), or app status (required apps, blacklisted apps), and get remediation details for any non-compliant devices. Devices can be geographically located and specific apps and devices can be remotely wiped.
- **Threat Protection**
  The suite protects mobile devices against malicious threats and unauthorized access to sensitive corporate information by utilizing antimalware and web browser protection. This helps protect mobile assets and provides compliance with internal and external security requirements. Device protection is enhanced by anti-theft protection where administrators can locate, lock, and wipe the device as needed. Protection is extended to the apps by defining and enforcing blacklists and whitelists.
- **Secure Content Distribution**
  The suite provides an easy way for enterprises to distribute content to end-user mobile devices. Administrators can distribute documents and multimedia content, in different file formats and apply appropriate corporate security policies at a per-file level. The suite supports updating and revoking content seamlessly.

MOBILE APPLICATION MANAGEMENT HIGHLIGHTS

Organizations that plan to implement employee-owned (BYOD) programs require the ability to target and control specific mobile business applications. The suite's app wrapping capability enables seamless and secure coexistence of personal and professional activities. Mobile Management Suite provides the capability to wrap a layer of security and policy management around any app, without requiring any coding. Symantec app-wrapping does not involve any SDK's or API's. Enterprises can wrap any in-house, third-party or Web apps like any other mobile app by creating and enforcing policies on a per-app basis. The suite automatically unpacks, updates and repacks the apps with a policy management layer prior to app distribution. This layer automatically enforces these policies at runtime on the device.

- Granular per-object policies for apps and content
- User authentication and re-authentication
- Data encryption (option to apply FIPS certified cryptographic algorithms)
- Whether the app is enabled to write data to local storage
- Whether off-line access is allowed
- Whether document sharing, copy/paste, or other APIs are enabled

MOBILE DEVICE MANAGEMENT HIGHLIGHTS

To support managing enterprise owned devices, Mobile Management Suite provides comprehensive mobile device management capabilities to facilitate scalable, secure, and integrated smartphone and tablet deployments. The suite allows IT to use a single solution to manage all mobile devices. Administrators can set, deploy, and update security settings such as passwords, remote lock and wipe, application, resource, and content restrictions over-the air, in near real-time without user intervention. Policy settings can be targeted to an individual user, device, or groups from the directory systems. The suite provides enterprise grade management with a scalable and mail server agnostic architecture and it supports distributed deployments with role-based access control. The suite provides exact details of enterprise mobile assets at all times by leveraging built-in dashboards, reports, and alerts. Comprehensive user, device, app, and profile details are available for additional custom reports as well.

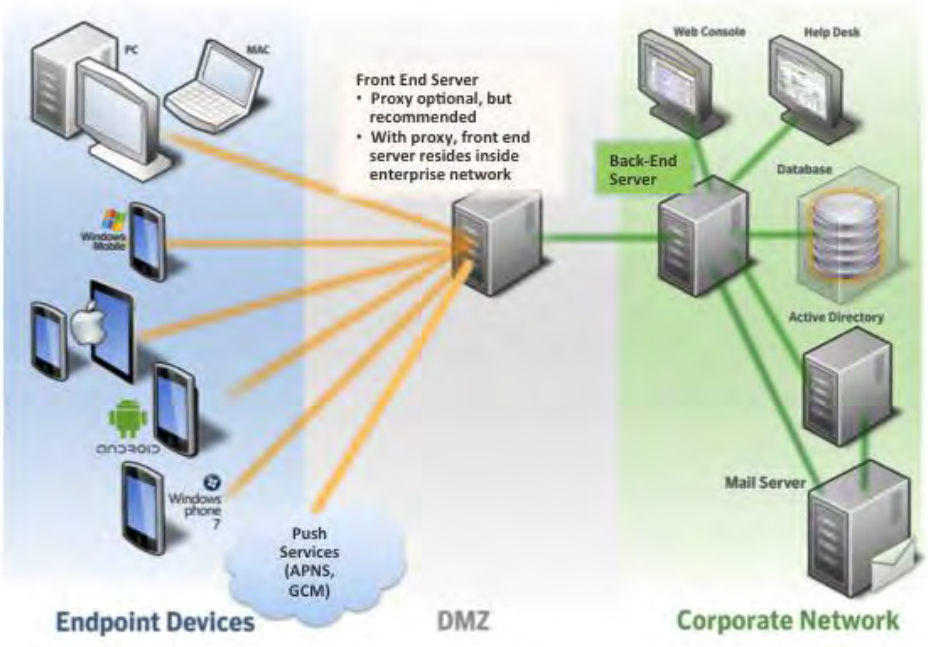
TRUSTED ECOSYSTEM: SYMANTEC™ SEALED PROGRAM

App Center supports an ecosystem of third-party app developers, enabling them to deliver their enterprise apps on mobile devices in way they can be centrally secured and protected. The Symantec™ Sealed Program makes it easy for third-party app developers to enable commercial apps for mobile protection without need for SDKs. The program allows mobile application developers to co-brand their apps and integrate Symantec's security and management

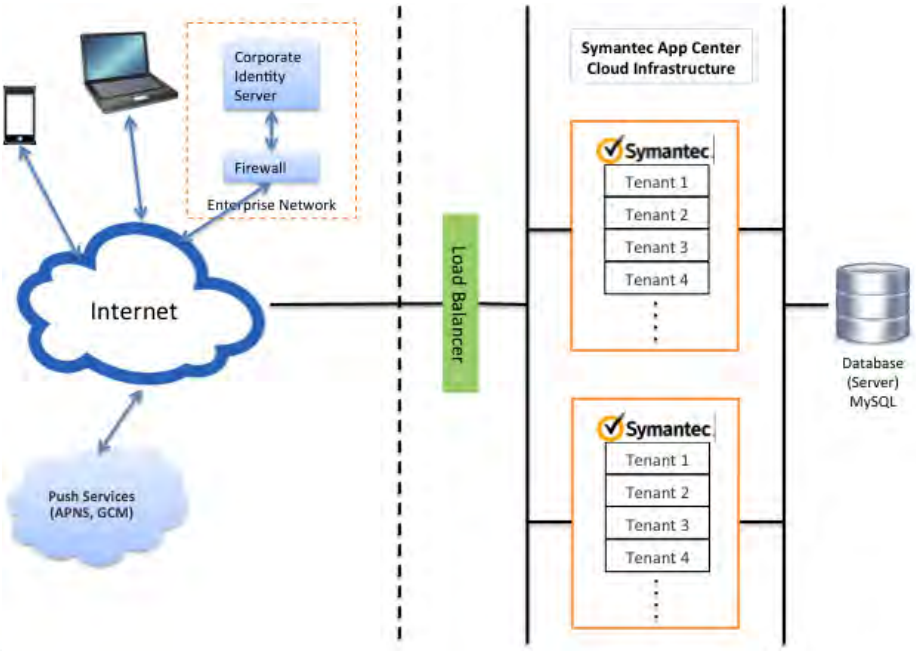
features, such as encryption, authentication, data loss prevention policies, and app policy distribution and revocation into their apps. IT organizations will be able to confidently deploy these apps with the same level of management, protection, and trust as in-house apps.

ARCHITECTURE

Symantec Mobile Management Suite: On-Premises Architecture



Symantec Mobile Management Suite: Cloud/SaaS Architecture



LICENSING

Symantec Mobile Management Suite is a subscription license sold per user per year. Licenses can be purchased for 12, 24 or 36 months.

8.12 VMWARE HORIZON

INTRODUCTION

The VMware Horizon Suite consists of a number of products. These products are also available as separate products. The products in the Horizon Suite are:

- Horizon Mirage (central management of desktops, local execution)
- Horizon View (central management of desktops, central execution)
- Horizon Workspace (workspace aggregator, provide access to desktops, apps and data)

Horizon Mobile (central management of mobile applications) is available as a free product included with Horizon Workspace and will be integrated in Horizon Workspace in a future release.

Horizon is also VMware's vision for End User Computing. In this vision, Horizon is the central component to provision applications, desktops, Windows applications, mobile applications, SaaS applications, and to provide the capability to sync data across all devices.

As the focus of this document is Enterprise Mobility Management, this paragraph will describe the capabilities of Horizon Workspace and Horizon Mobile.

The key features of **Horizon Workspace** are:

Single End-user Workspace

- Easy Access to Enterprise Data, Apps, Services, Virtual Desktops

- Single context-based catalog
- Single Sign On
- One-click Access and self-service to application assignment

Centralized IT Management

- Federated Identity Management with Active Directory integration
- Centralized Entitlement Management
- Unified Policies Management
- Context Management File Sharing
- Anytime, anywhere access
- Offline & online data access
- High-fidelity doc previews
- Document versioning, commenting and auditing

Enterprise-Grade Security

- Endpoint registration & wipe
- Document sandbox
- Encryption on mobile devices
- App passcode policy
- Support RSA Multifactor authentication

Integration with Horizon View

- Easy access to Virtual Desktops & App Services via Horizon View
- SSO brokering user to available desktops based on entitlement policy
- Leverage remote protocol to access View from any HTML5 browser

At this time, Horizon Workspace enables IT to help deploy Enterprise-approved third party applications. This means that only app links to the mobile app store for app installation can be provisioned (Apple store or Google Play store). Referred apps link to the mobile app store, Horizon Workspace does not open the installed applications.

The key features of **Horizon Mobile** are:

Control and Customize Enterprise Mobile Workspaces

- Easy provisioning of applications and enterprise services to employee devices through a dedicated workspace.
- Native application support within the corporate workspace enables any Android application file package (APK), including ones developed in-house, to be deployed to an employee's corporate workspace without modification.
- Over the air application distribution and updates.
- Preconfigure application preferences from Horizon Mobile Manager before distributing applications to employees.

Securely Manage Corporate Assets on Mobile Devices

- Protects corporate data with enterprise-grade security by strictly isolating personal and corporate assets through two distant operating system and file systems.
- Provides a Web-based tool for administrators to create group based security policies, certificate management, monitor device inventory and obtain device diagnostic information.

- Provides full encryption of all corporate data, remote lock and wipe, rootkit detection, and password enforcement.

Embrace Employees' Mobile Way of Working

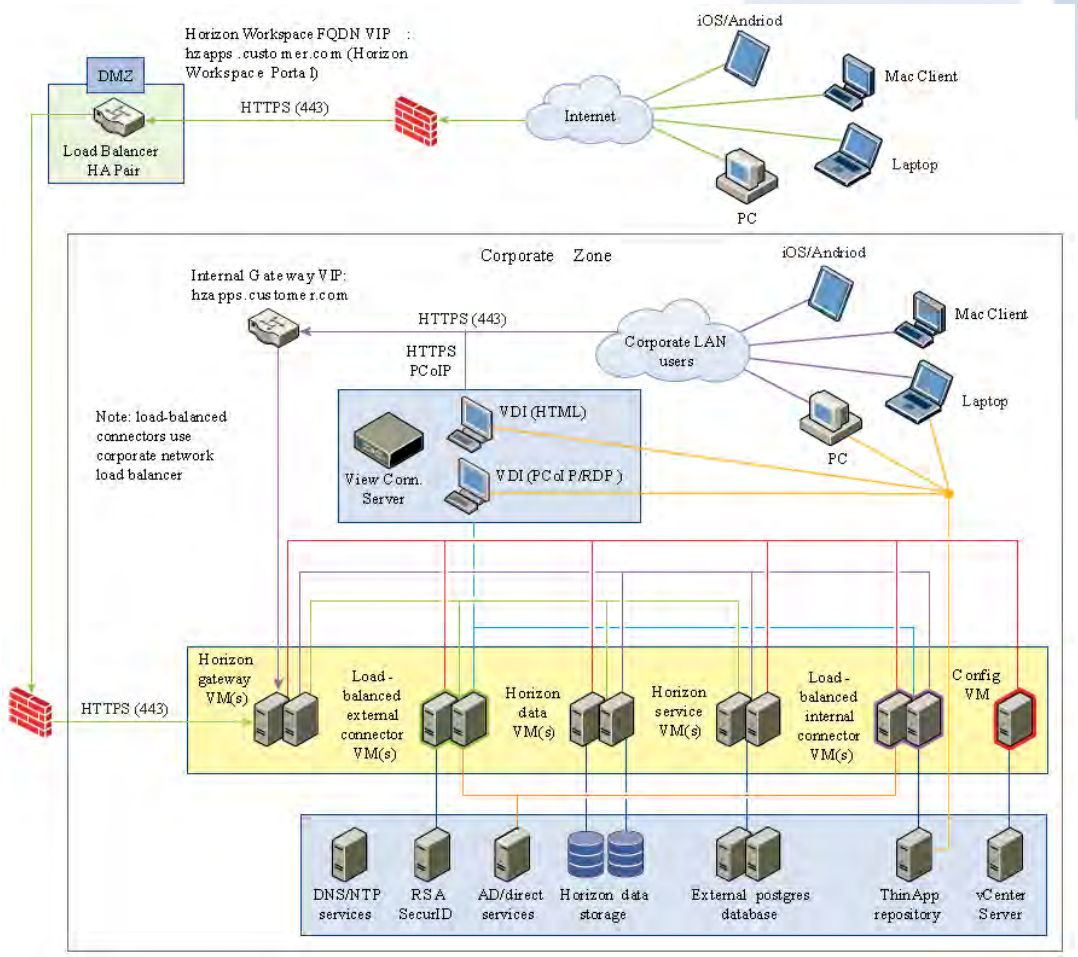
- Enables employees to use their device of choice for both personal life and work, while protecting their privacy.
- Empowers users with full access to enterprise services while they are on the go.
- Gives employees a consistent, easy-to-use native mobile experience across devices, regardless of model.

ARCHITECTURE

Horizon Workspace is a multiple virtual machine vApp, distributed as an Open Virtualization Archive (OVA) file. You can deploy the vApp to vCenter. The vApp includes several virtual appliances:

- Configurator VM
  - Horizon Workspace is configured first with this virtual appliance. The configurations made with the Configurator are distributed to the other virtual appliances in the vApp.
- Gateway VM
  - The Horizon Workspace Gateway Virtual Appliance is the single endpoint for all end user communication. User requests come to the gateway-va, which then routes the request to the appropriate virtual appliance.
- Service VM
  - Horizon Workspace Manager handles ThinApp package synchronization and gives access to the Administrator Web interface, from which users, groups, and resources can be managed.
- Connector VM
  - The Connector provides the following services: user authentication (identity provider), directory synchronization, ThinApp-catalog loading, and View pool synchronization.
- Data VM
  - The Horizon Workspace Data Virtual Appliance controls the file storage and sharing service, stores users' data (files), and synchronizes users' data across multiple devices.

Failover and redundancy can be achieved by adding multiple virtual machines of the same type in Horizon Workspace vApp.



The infrastructure requirements for Horizon Workspace are:

- vCenter (5.x)
- ESXi (4.1, 5.0, 5.1)
- Active Directory (Win 2008 R2)
- Database (Horizon Service)
    - Internal DB - postgres
    - External DB – postgres

VMware Horizon Mobile is also a vApp, distributed as an OVA file. Horizon Mobile enables enterprises to securely provision and manage a corporate mobile workspace on employees' Android smartphones in isolation from their personal environment. This dual persona solution enables enterprises to embrace employees' preferred mobile devices while maintaining the security, compliance and manageability enterprises require. Horizon Mobile provides a wide range of features to enhance productivity by creating a purpose-built and preconfigured native mobile workspace based on employee responsibilities that is tied to the user, not the device.

The key components in a VMware Horizon Mobile environment are:

- VMware Horizon Mobile Manager virtual appliance
- VMware Ready mobile device
- VMware Switch application
- Base workspace image

After a user installs VMware Switch on a VMware Ready mobile device, a base workspace image together with a policy can be deployed to the mobile device. The user then has two environments on the smartphone; one for personal use and one for business use. The business environment is managed by the Horizon Mobile Manager and can be locked down or remotely whipped when necessary.

LICENSING

Licensing of users is according to which Horizon bundle or suite you purchase:

Bundle or Suite	Components	Type of License
Horizon View	Horizon View ThinApp Workstation * vSphere Desktop vCenter Desktop	Concurrent User
Horizon Mirage	Horizon Mirage ThinApp Workstation * Fusion Pro	Named User
Horizon Workspace	Horizon Workspace ThinApp Workstation *	Named User

Bundle or Suite	Components	Type of License
	Horizon Mobile for Android	
Horizon Suite	All three smaller bundles: Horizon View Horizon Mirage Horizon Workspace	Named User

* In all Horizon bundles and the suite, VMware Workstation is licensed for the creation of virtual machines for the ThinApp capture-and-build process. Workstation is not licensed for creating virtual machines for users. VMware Fusion Pro in the Horizon Mirage bundle is intended for the creation of virtual machines for users, and Horizon Mirage can manage those Fusion virtual machines.

9. EMM FEATURES COMPARISON

9.1 INTRODUCTION

It is important to understand that comparing product features is the last step in the MobileIT decision tree. Vision, Strategy and Technology are the former steps. Each EMM product has its own functionality and feature set. In addition, due to platform restrictions or security features, not all features are supported on all mobile platforms. It's key to have an overview of the vendors, solutions and their functionality. Some vendors offer complete and comprehensive sets of functionality, while others are focused on delivering a smaller solution set with specific functionality. Both scenarios are good; it all depends on what kind of functionality you're looking for. Keep the strategic questions mentioned in chapter 6 in mind!

Below you will find an overview of the various vendors, their solutions and the functionality they're offering at a very high level. We've done our best to be truthful and accurate in investigating and writing down the different features. When you see the need for improvements or fixes, please let us know.

9.2 COMPARE MATRIX, QUICK REFERENCE

There are many vendors in the "Enterprise Mobility Management space". The diagram below gives an overview of the **focus** of the various Enterprise Mobility Management (**EMM**) software **vendors**. This diagram has nothing to do with the (possible) discussion which vendor provides the most and the best functionality and features. A complete overview of the **features** and **functionality** is available in chapter 9.6 – Compare Matrix, Features.

Category	AirWatch EMM Suite	Appsense MobileNow	Citrix XenMobile	Good	MaaS360 by Fiberlink	Microsoft Exchange ActiveSync	Microsoft Intune	MobileIron	Symantec MM Suite	VMware Horizon
Mobile Device Management	●	●	●	●	●	○	●	●	●	●
Mobile Application Management	●	●	●	●	●	○	○	●	●	○
Mobile Information Management	●	●	●	●	●	○	○	●	●	●
Mobile Expense Management	●	○	○	●	●	○	○	●	●	○
Secure Mail Client	●	●	●	●	●	○	○	●	●	●
Secure Data, FileSync	●	●	●	●	●	○	○	●	●	●
Secure Web Browser	●	●	●	●	●	○	○	●	●	○

9.3 ROADMAP AND FUTURE ADDITIONS

We plan to add more feature details on the currently named vendor solutions and want to add new solutions where applicable. If you have any comments, corrections, or suggestions for improvements of this document, we want to hear from you!
Please send e-mail to Peter Sterk (pst@pqr.nl) or Ruben Spruijt (rsp@pqr.nl)

9.4 PRODUCT VERSION

This detailed feature compare matrix is based on the following products and versions:

Product	Version	Release date
AirWatch Enterprise Mobility Management Suite	6.3	Q1 2013
AppSense EMM Suite	2.0	January 2013
Citrix XenMobile	8.5	May 2013
Good for Enterprise	2.2.0	n/a
MaaS360 by Fiberlink	n/a	n/a
Microsoft Exchange ActiveSync	14.1	August 2010
Microsoft Intune	4.0	January 2013
MobileIron	5.6	March 2013
Symantec Mobile Management Suite	n/a	October 2012
VMware Horizon Workspace	1.0	March 2013
VMware Horizon Mobile	1.3	December 2012

9.5 FEATURE COMPARE MATRIX

	EMM solutions and features
Goal:	Detailed description of features
Requirements:	Hands-on-experience, vendor involvement
Result:	Whitepaper
Method of Execution:	Hands-on experience, read articles, communicate with vendors and discuss with colleagues

Used legend:

√=Applicable; X=Not applicable;--Not needed; ~=It depends; #= Under investigation of PQR;

A green √ or red X has nothing to do with advantage or disadvantage of a solution. It just presents the availability of the functionality. Note: It's out of scope for this whitepaper to explain the 'It depends' remarks'.

9.6 COMPARE MATRIX, FEATURES

Category	AirWatch EMM Suite	AppSense EMM Suite	Citrix XenMobile	Good for Enterprise	Microsoft Intune	MobileIron	Symantec MM Suite	Remarks
Supported (mobile) platforms								
Android 2.2	√	√	√	√	√	√	√	
Android 3.x	√	√	√	√	√	√	√	
Android 4.x	√	√	√	√	√	√	√	
Android 4.x, support for Samsung SAFE		√						
Apple iOS 4.x	√	√	√	√	√	√	√	
Apple iOS 5.x	√	√	√	√	√	√	√	
Apple iOS 6.x	√	√	√	√	√	√	√	
Apple MAC OS X	√	~	~	X	X	√	X	~ AppSense: DataNow only
BlackBerry 7.x	√	X	√	√	X	√	√	
BlackBerry 10	√	X	√	X	X	√	X	
Linux	X	~	~	X	X	X	X	~ Appsense: DataNow only
Symbian	√	X	√	√	X	√	√	
Windows Mobile 6.x	√	X	√	√	√	√	√	
Windows Phone 7.5	√	~	√	√	√	√	√	~ AppSense: DataNow only

Category	AirWatch EMM Suite	AppSense EMM Suite	Citrix XenMobile	Good for Enterprise	Microsoft Intune	MobileIron	Symantec MM Suite	Remarks
Windows Phone 8.x	√	~	√	X	√	√	√	~ AppSense: DataNow only
Windows XP SP3	X	~	√	X	√	X	X	~ AppSense: DataNow only
Windows 7	X	~	√	X	√	X	X	~ AppSense: DataNow only
Windows 8	√	~	√	X	√	√	X	~ AppSense: DataNow only
Windows RT	√	~	X	X	√	√	√	~ AppSense: DataNow only
iOS - Supports Apple MDM device management API's:	√	√	√	√	√	√	√	
WP8 – Supports Exchange Active Sync management policies	#	#	#	#	#	√	#	
Mobile Device Management - *(Not all features are supported on all Mobile platforms)*								
Block noncompliant OS platforms and versions	√	√	√	√	X	√	√	
Block noncompliant applications	√	√	√	√	X	√	√	
Restrict access from noncompliant devices,	√	√	√	√	X	√	√	
Max number of devices per user, for instance 5.	√	√		√	√	√	X	Value is configurable.
Application whitelisting	√	~	√	√	X	√	√	~ Android only
Application blacklisting	~	~	~	~	~	~	~	~ Android only
Send alerts for policy violations	√	√	√	√	X	√	√	
Enforce password complexity	√	√	√	√	√	√	√	
Enforce password duration	√	√	√	√	√	√	√	

Category	AirWatch EMM Suite	AppSense EMM Suite	Citrix XenMobile	Good for Enterprise	Microsoft Intune	MobileIron	Symantec MM Suite	Remarks
Enforce password expiration	√	√	√	√	√	√	√	
Enforce password lock after time of inactivity	√	√	√	√	X	√	√	
Remote lock	√	√	√	√	X	√	√	
Remote wipe - full	√	√	√	√	√	√	√	
Remote wipe – selective	√	√	√	√	X	√	√	
Certificate-based authentication	√	√	√	√	X	√	√	
Certificate distribution	√	√	√	√	X	√	√	
Certificate revocation	√	√	~	√	X	√	√	
Manage firewall on device, if applicable	X	X	√	X	√	√	~	~ Windows Mobile only
Manage antivirus on device, if applicable	~	X	X	X	√	√	~	~ Windows Mobile & Android only
Manage VPN on device, if applicable	√	√	√	√	X	√	~	~ iOS only
Monitor, audit and report message flows	√	√	√	√	X	√	X	
Application Inventory	√	√	√	√	√	√	√	
Application distribution through enterprise app store	√	√	√	√	√	√	√	
Integration with Apple Volume Purchase Program	√	√	√	√	X	√	√	
Integration with Google Playstore volume licensing	X	X	X	X	X	X	X	Not available/supported by Google today
Over-the-Air updates for applications	√	√	√	√	√	√	√	

Category	AirWatch EMM Suite	AppSense EMM Suite	Citrix XenMobile	Good for Enterprise	Microsoft Intune	MobileIron	Symantec MM Suite	Remarks
Over-the-Air updates for mobile OS	~	√	~	X	X	X	~	~ Windows Mobile only
Backup and restore mobile devices	√	√	~	√	X	√	X	~ Backup/Restore for corporate data possible
Support for Role Based Access Administration	√	√	√	√	√	√	√	
Audit logging available in management console	√	√	√	X	#	√	√	
Block external memory in mobile devices, if applicable	√	√	√	√	X	√	√	
Configure wireless networks on the device	~	√	~	~	#	~	~	~ iOS & Windows Mobile only
Limit wireless networks on the device	~	~	~	~	X	~	~	Android only
Prevent screen captures for specific apps or data	√	√	√	X	X	√	X	
Locate devices	√	√	√	X	#	√	√	
Schedule deployments to devices	√	X	√	X	√	√	~	~ Windows Mobile only
Specify conditions for deployments to devices	√	√	√	√	√	√	√	
Inventory carrier network	√	√	√	√	~	√	√	~ iOS only
Inventory mobile country code	√	√	√	√	~	√	√	~ iOS only
Inventory network code	√	√	√	√	~	√	√	~ iOS only
Android – Detect rooted devices	√	√	√	√	X	√	√	
Enroll devices in bulk	√	√	√	√	X	√	X	
Enroll devices by user	√	√	√	√	√	√	√	

Category	AirWatch EMM Suite	AppSense EMM Suite	Citrix XenMobile	Good for Enterprise	Microsoft Intune	MobileIron	Symantec MM Suite	Remarks
Enroll devices by e-mail	√	√	√	√	√	√	√	
Enroll devices trough native app	√	√	√	X	X	√	√	
Mobile Application Management *(- Not all features are supported on all platforms)*								
Deploy Android Apps	√	√	√	√	√	√	√	
Deploy Android Google Playstore apps	√	√	√	√	√	√	√	
Deploy Apple Apps	√	√	√	√	√	√	√	
Deploy Apple App Store Apps	√	√	√	√	√	√	√	
Deploy MAC OS X Apps	~	X	√	X	X	~	X	
Deploy Windows Apps	√	X	√	X	√	X	X	
Deploy Windows Store Apps	√	X	√	X	√	√	X	
Deliver Windows Apps	√	X	√	X	√	X	X	
Deliver Windows Phone Store apps	√	X	√	X	√	√	X	
Push mandatory apps to devices	√	√	√	√	√	√	√	
Create categories of apps	√	√	√	X	√	√	√	
Create list of suggested apps	√	√	√	√	√	√	√	
Support for third-party application stores	√	√	√	√	√	√	√	
Application wrapping	√	√	√	√	X	√	√	

Category	AirWatch EMM Suite	AppSense EMM Suite	Citrix XenMobile	Good for Enterprise	Microsoft Intune	MobileIron	Symantec MM Suite	Remarks
Application wrapping with third-party solution	~	X	~	X	X	X	√	
Deploy managed apps in one container	~	X	√	X	X	X	X	
Deploy managed apps in different containers	√	√	√	√	X	√	√	
Encryption of containers	√	√	√	√	X	√	√	
Prevent data leakage to unmanaged apps	√	√	√	√	X	√	√	
Control data exchange between managed apps	√	√	√	√	X	√	√	
Verify application origin	√	√	√	X	X	√	√	Only true if supported by Mobile Operation System
Single Sign On for managed applications	√	√	√	√	X	√	√	
Application policies	√	√	√	√	X	√	√	
- Set minimum mobile OS platform version for apps	√	√	√	√	X	√	√	
- Set maximum mobile OS platform version for apps	√	√	√	√	X	√	X	
- Exclude devices from specific apps	√	√	√	X	X	√	X	
- Require logon on application start	√	√	√	√	X	√	√	
- Require explicit logon on application start	√	√	√	√	X	√	√	
- Require WiFi on application start	√	X	√	X	X	X	X	
- Require network on application start	√	√	√	X	X	X	√	
- Require device passcode	√	√	√	X	X	√	√	

Category	AirWatch EMM Suite	AppSense EMM Suite	Citrix XenMobile	Good for Enterprise	Microsoft Intune	MobileIron	Symantec MM Suite	Remarks
- Block jailbroken devices	√	√	√	√	X	√	√	
Android - Application whitelisting	√	√	√	√	X	√	√	
Android - Application blacklisting	√	√	√	√	X	√	√	
iOS - Application whitelisting	√	X	√	√	X	√	√	
iOS - Application blacklisting	√	√	√	√	X	√	√	
WP8 - Application whitelisting	X	X	X	X	X	X	X	
WP8 - Application blacklisting	X	X	X	X	X	X	X	
Mobile Information Management - *(Not all features are supported on all platforms)*								
Manage personal data on corporate device	√	√	X	√	X	√	X	
Manage corporate data on personal device	√	√	√	√	X	√	√	
Wipe personal data from corporate device	√	√	√	√	X	√	√	Through full device wipe
Wipe corporate data on personal device	√	√	√	√	X	√	√	
Prevent data leakage to unmanaged apps	√	√	√	√	X	√	√	
Control data exchange between managed apps	√	√	√	√	X	√	√	
Encrypt local data	√	√	√	√	√	√	√	Only true if supported by Mobile Operation System
Allow access to information based on location	√	√	√	X	X	√	X	
Distribute content to mobile devices	√	√	√	X	√	√	√	

Category	AirWatch EMM Suite	AppSense EMM Suite	Citrix XenMobile	Good for Enterprise	Microsoft Intune	MobileIron	Symantec MM Suite	Remarks
Distribute content to mobile devices with third-party apps	√	√	X	√	X	√	√	e.g. Accellion
Distribute content to mobile devices using encryption	√	√	√	X	√	√	√	
Distribute content to mobile devices with third-party apps using encryption	√	√	X	√	X	√	√	
Send alerts for policy violations	√	√	√	√	X	√	√	
Block cut/copy/paste between personal and corporate apps	√	√	√	√	X	√	√	
Secure access to on-premises webservices	√	√	√	√	X	√	√	
Secure access to on-premises Microsoft Sharepoint	√	√	√	√	X	√	√	
Android – media encryption	√	√	√	√	X	√	√	
Distribute Adobe PDF files to device	√	√	√	X	X	√	√	
Distribute image files to device (PNG, BMP, JPEG)	√	√	√	X	X	√	√	
Distribute Microsoft Office files to device	√	√	√	X	X	√	√	
Check if file exist, otherwise copy the file	√	√	~	X	X	√	X	
Configure attributes for the file (readonly, hidden)	√	√	~	X	X	X	X	
Provide description for the file	√	√	~	X	X	X	√	
Specificy destination location for the file	~	√	~	X	X	X	√	~ Android and Windows Mobile only
Block Cloud services (e.g. iCloud)	√	√	√	√	~	√	√	~ Apple iOS only
Mobile Expense Management - *(Not all features are supported on all platforms)*								

Category	AirWatch EMM Suite	AppSense EMM Suite	Citrix XenMobile	Good for Enterprise	Microsoft Intune	MobileIron	Symantec MM Suite	Remarks
Monitor roaming usage	√	X	X	√	X	√	X	
Limit roaming usage	√	X	√	√	X	√	X	Only true if supported by Mobile Operation System
Prevent roaming usage	√	X	~	√	X	√	~	Only true if supported by Mobile Operation System
Send alerts for policy violations	√	X	√	√	X	√	X	
Secure email - *(Not all features are supported on all platforms)*								
Supports native app	√	√	√	X	√	√	√	
With third party app	√	√	√	√	X	√	√	
Encrypt attachments	√	√	√	√	X	√	X	
Block specific attachments	√	√	√	√	X	√	X	
Support Exchange Active Sync device access rules	√	√	√	√	√	√	√	
Containerization of email profiles native mail client	√	√	√	X	X	√	√	
Containerization of email profiles with third-party mail client	√	√	√	√	X	√	√	
Prevent e-mail forwarding	√	√	√	X	X	√	√	
Prevent e-mail forwarding based on content / attachments	√	X	√	X	X	X	X	
Prevent e-mail forwarding based on user or user group		X		X	X	√	#	
Prevent e-mail forwarding based on device or device group	#	X	#	X	X	√	#	
Configure e-mail profiles on the device	√	√	√	√	√	√	√	

Category	AirWatch EMM Suite	AppSense EMM Suite	Citrix XenMobile	Good for Enterprise	Microsoft Intune	MobileIron	Symantec MM Suite	Remarks
Microsoft Exchange Server support	√	√	√	√	√	√	√	
Microsoft Office 365 support	√	√	√	√	√	√	√	
Google Gmail support	√	√	√	X	X	√	√	
IBM Lotus Notes/Domino support	√	√	√	√	X	√	√	
IMAP support	√	X	√	√	√	√	√	
Share (specific) details of corporate contacts with personal contacts	~	X	X	√	X	X	X	
Platform / infrastructure								
Cloud (SaaS) service available	√	√	√	X	√	√	√	
On-premises solution, no inbound firewall rules necessary	X	X	X	√	X	X	X	
Integration with Microsoft System Center 2012	√	X	X	X	√	√	√	
High available deployment possible	√	√	√	√	X	√	√	
Disaster recovery techniques available	√	√	√	√	X	√	√	
Support for over 5.000 devices	√	√	√	√	√	√	√	~ Microsoft use ‘Users’, not devices
Support for over 10.000 devices	√	√	√	√	~	√	√	~ Microsoft use ‘Users’, not devices
Support for over 20.000 devices	√	√	√	√	~	√	√	~ Microsoft use ‘Users’, not devices
Active Directory supported	√	√	√	√	√	√	√	
LDAP supported	√	√	√	√	√	√	√	

Category	AirWatch EMM Suite	AppSense EMM Suite	Citrix XenMobile	Good for Enterprise	Microsoft Intune	MobileIron	Symantec MM Suite	Remarks
Windows Server 2003 support	X	X	√	√	~	~	X	~ No need for on-premises server
Windows Server 2008 support	√	X	√	√	~	~	√	~ No need for on-premises server
Windows Server 2008 R2 support	√	√	√	√	~	~	√	~ No need for on-premises server
Windows Server 2012 support	X	X	√	√	~	~	√	~ No need for on-premises server
Support for two-factor authentication	√	√	X	√	X	√	X	
Support for multi-factor authentication	X	√	X	√	X	√	X	
Licensing								
Licensed per user	X	√	√	X	√	√	√	
Licensed per device	√	√	√	√	X	√	~	
Subscription license	√	√	√	~	#	√	√	
Perpetual license	√	√	√	~	#	√	X	
First year support and maintenance included in license	√	√	X	√	#	√	√	
Software Maintenance is mandatory for 1st year	~	√	√	√	#	√	√	
24 x 7 support included in license	~	√	~	X	#	~	√	~ Available option
Grace period	√	√	√	√	#	X	√	
Free for personal usage (FFPU)	X	X	X	X	X	~	X	
Free trial period	√	√	√	#	√	√	#	

Category	AirWatch EMM Suite	AppSense EMM Suite	Citrix XenMobile	Good for Enterprise	Microsoft Intune	MobileIron	Symantec MM Suite	Remarks
Free for students at educational institutions	#	X	#	#	#	√	#	
Various								
Open Mobile Alliance device management v1.2 supported	√	X	~	X	X	X	~	~ Windows Mobile only
Support and Community								
Certification program for ISVs	X	√	√	X	X	√	√	
Public and active community forum	X	√	X	X	X	√	√	
Official training classes available	√	√	√	X	X	√	√	
Official certification program, VUE or Prometric	X	X	X	X	X	√	√	
EMM technology stack is proven, the solution is being used for 1+ year in enterprise production environments. 10K+ endpoint, various deployment scenarios	X	X	√	X	X	√	√	
10+ of public available enterprise (10K CCU) references in EU using EMM technology stack	X	X	X	X	X	√	X	
10+ of public available enterprise (10K CCU) references in US using EMM technology stack	X	X	X	X	X	√	X	
Vendor created reference design for enterprise architecture, public availa-			√			~		~ MobileIron: Customers only

Category	AirWatch EMM Suite	AppSense EMM Suite	Citrix XenMobile	Good for Enterprise	Microsoft Intune	MobileIron	Symantec MM Suite	Remarks
ble								~ AppSense: Customers and Partners
SMB Reference Architecture , public available		~	√			~		~ MobileIron: Customers only ~ AppSense: Customers and Partners

10. CHANGE LOG

Date June 2013; Document version 1.1

- Removed Gartner Hypecycles (chapter 6.1, 6.2 and 6.3)
- Changed "EMM technology stack is proven, the solution is being used for 1+ year in enterprise production environments. 10K+ endpoint, various deployment scenarios" for Symantec Mobile Management Suite
- Change mobile client platform support "MAC OS X", "Windows 8" and "Windows RT" for AirWatch Enterprise Mobility Management Suite
- Changed "Support for two-factor authentication" for AirWatch Enterprise Mobility Management Suite
- Changed "Official training classes available" for AirWatch Enterprise Mobility Management Suite
- Added "MaaS360 by Fiberlink" to chapter 8
- Added "MaaS360 by Fiberlink" to table in chapter 4.15
- Added "MaaS360 by Fiberlink" to table in chapter 9.2
- Added "MaaS360 by Fiberlink" to table in chapter 9.4
- Changed "AppSense DataNow" to "AppSense EMM Suite"
- Changes various features for AppSense EMM Suite
- Removed references to "Microsoft System Center Configuration Manager required" for some "Windows Intune" features; if additional software is required this feature is valued "**X**=Not applicable"
- Added Cor Reinhard to the A-Team (PQR) members

Date May 2013; Document version 1.0

- Awesome, the initial version; feedback? pst@pqr.nl or rsp@pqr.nl ☺

11. APPENDIX: A-TEAM (PQR) MEMBERS

Henk Hoogendoorn has experience in the ICT for almost 15 years now. He is working as a Consultant & Microsoft Certified Trainer (MCT) at PQR. His specialty is centering on Device Management and User Environment Management (i.e. management of servers, desktops, mobile devices and applications), focusing in keeping it simple and effective. Henk is active on several blog sites as a writer on Microsoft System Center solutions. He shares his knowledge on Microsoft TechNet Forums. Henk can be reached at hho@pqr.nl or twitter.

Marcel van Klaveren (1978) started his career as System Engineer and has over 15 years of experience in the IT business. During these years, Marcel has developed several fields of expertise and certifications like, Microsoft Certified IT Professional Enterprise Messaging Administrator 2010 (MCITP-EA Exchange 2010), Symantec Technical Specialist (STS) on Enterprise Vault and VMware Certified Professional (VCP). In his function as messaging consultant at PQR, Marcel advises, designs and migrates IT infrastructures.

Anton van Pelt (1984) is a Technical Consultant at PQR. Anton his focus is on Application and Desktop Delivery solutions. Nevertheless, his interests are going much further than this what gives him a broad knowledge in complex IT environments. Anton advises, designs, implements and migrates advanced ICT-infrastructures. Having achieved the highest certifications of its most important partners, Anton is a Citrix Certified Integration Architect (CCIA), a Microsoft Certified Systems Engineer (MCSE) and a RES Certified Professional (RCP). Anton is awarded as a RES Software Value Professional (RSVP). Follow Anton on twitter or contact him via email

Sven Huisman (1977) studied Information Management in Utrecht. He started his career as system engineer and meanwhile he has over 10 years of experience in the IT business. He is one of PQR's technical Consultants, focusing on Application and Desktop Delivery, hardware and software virtualization. Sven advises, designs, implements and migrates advanced ICT-infrastructures. Having achieved the highest certifications of its most important partners, Sven is a Citrix Certified Enterprise Administrator (CCEA), a Microsoft Certified Systems Engineer (MCSE) and a VMware Certified Professional (VCP). Sven is awarded as VMware vExpert. You can reach Sven at shu@pqr.nl or twitter.

Erik van Veenendaal (1982) is a technical consultant at PQR. Erik started his IT career as a system engineer, and meanwhile has over 10 years of experience in complex ICT infrastructures. His focus is Application and Desktop Delivery solutions including User Environment Management. Erik is analytical and has a broad knowledge he can utilize within advises, designs, implementations and migrations of advanced ICT-infrastructures. Erik has reached certification levels like a Citrix Certified Integration Architect (CCIA), Microsoft Certified Solutions Associate (MCSA): Windows Server 2012, RES Workspace manager Certified Professional (RPFCP). You can reach Erik at eve@pqr.nl or twitter.

Cor Reinhard is an IT Professional and Microsoft Certified trainer offering a wide base of IT skills combined with over 12 years of experience as an IT Consultant and Architect. Cor is consistently recognized for his deep knowledge of Microsoft technology and shares this knowledge via various forum like congresses, seminars, his personal blog and training sessions. Cor his main areas of focus are Unified Communications, Messaging, Public Cloud and Active Directory Services.

PQR B.V.
Rijnzathe 7
3454 PV De Meern
The Netherlands

Tel: +31 (0)30 6629729
Fax: +31 (0)30 6665905
E-mail: info@pqr.nl
www.PQR.com