## 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. **Enterprise Mobility** ................................................................................................................... 8  
   3.1 Enterprise Mobility as one of the top priorities ....................................................................... 8  
   3.2 Consumerization of IT ............................................................................................................. 8  
   3.3 Application delivery: 3-2-1 and action! .................................................................................... 9  
   3.4 IT as a Service and tomorrow’s IT organization .................................................................... 12  
   3.5 Enterprise Mobility Management 2014 by Jack Madden ....................................................... 13  

4. **Mobile IT Strategy** ................................................................................................................... 14  
   4.1 Data Management .................................................................................................................... 14  
   4.2 Applications ............................................................................................................................. 14  
   4.3 Devices .................................................................................................................................... 14  
   4.4 Secure Access and Networking ............................................................................................. 15  
   4.5 Policies and regulations .......................................................................................................... 15  
   4.6 Generic .................................................................................................................................... 15  

5. **Enterprise Mobility Management** ........................................................................................ 17  
   5.1 Introduction ............................................................................................................................ 17  
   5.2 Mobile Device Management ................................................................................................... 17  
   5.3 Mobile Application Management ........................................................................................... 18  
   5.4 Mobile Information Management .......................................................................................... 19  
   5.5 Mobile Expense Management ............................................................................................... 20  
   5.6 Secure email ............................................................................................................................ 20  
   5.7 Secure Data, Enterprise FileSync .......................................................................................... 21  
   5.8 Secure Web browsers ............................................................................................................. 21  

6. **Vendors and their EMM Solutions** .......................................................................................... 22  
   6.1 Introduction ............................................................................................................................ 22  
   6.2 AirWatch by VMware ........................................................................................................... 22  
   6.3 AppSense EMM Suite .............................................................................................................. 26  
   6.4 BlackBerry Enterprise Service 10 (BES10) ............................................................................. 30  
   6.5 Citrix XenMobile ................................................................................................................... 34  
   6.6 Cortado Corporate Server .................................................................................................... 37
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.7</td>
<td>Good for Enterprise</td>
<td>40</td>
</tr>
<tr>
<td>6.8</td>
<td>IBM MaaS360</td>
<td>44</td>
</tr>
<tr>
<td>6.9</td>
<td>Microsoft Exchange ActiveSync</td>
<td>49</td>
</tr>
<tr>
<td>6.10</td>
<td>Microsoft Enterprise Mobility Suite</td>
<td>50</td>
</tr>
<tr>
<td>6.11</td>
<td>MobileIron</td>
<td>56</td>
</tr>
<tr>
<td>6.12</td>
<td>Symantec Mobile Management Suite</td>
<td>58</td>
</tr>
<tr>
<td>6.13</td>
<td>VMware Horizon</td>
<td>62</td>
</tr>
<tr>
<td>7.</td>
<td>EMM features Comparison</td>
<td>68</td>
</tr>
<tr>
<td>7.1</td>
<td>Introduction</td>
<td>68</td>
</tr>
<tr>
<td>7.2</td>
<td>Comparison Matrix, Quick reference</td>
<td>69</td>
</tr>
<tr>
<td>7.3</td>
<td>Roadmap and Future additions</td>
<td>69</td>
</tr>
<tr>
<td>7.4</td>
<td>Product Version</td>
<td>70</td>
</tr>
<tr>
<td>7.5</td>
<td>Feature Compare Matrix</td>
<td>70</td>
</tr>
<tr>
<td>7.6</td>
<td>Compare Matrix, Features</td>
<td>71</td>
</tr>
<tr>
<td>8.</td>
<td>Change Log</td>
<td>85</td>
</tr>
<tr>
<td>9.</td>
<td>Appendix: A-Team (PQR) members</td>
<td>87</td>
</tr>
</tbody>
</table>
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 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 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 have 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 email to Peter Sterk (pst@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
email: info@pqr.nl ; Web: 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-premises to cloud management, without processes getting complex. Simplicity in ICT, that is 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, The Netherlands, and has over 100 employees. In fiscal year 2012/2013 posted sales of € 87.6 million and a net after tax profit of € 2.7 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!

<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
<th>Contact</th>
<th>Role</th>
<th>Twitter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Henk Hoogendoorn</td>
<td>Consultant PQR</td>
<td><a href="mailto:hho@pqr.nl">hho@pqr.nl</a></td>
<td>Writer</td>
<td>@henkhoogendoorn</td>
</tr>
<tr>
<td>Marcel van Klaveren</td>
<td>Consultant PQR</td>
<td><a href="mailto:mkv@pqr.nl">mkv@pqr.nl</a></td>
<td>Writer</td>
<td>@itguru3</td>
</tr>
<tr>
<td>Anton van Pelt</td>
<td>Consultant PQR</td>
<td><a href="mailto:ape@pqr.nl">ape@pqr.nl</a></td>
<td>Writer</td>
<td>@antonvanpelt</td>
</tr>
<tr>
<td>Sven Huisman</td>
<td>Consultant PQR</td>
<td><a href="mailto:shu@pqr.nl">shu@pqr.nl</a></td>
<td>Writer</td>
<td>@svenh</td>
</tr>
<tr>
<td>Erik van Veenendaal</td>
<td>Consultant PQR</td>
<td><a href="mailto:eve@pqr.nl">eve@pqr.nl</a></td>
<td>Reviewer</td>
<td>@evveenendaal</td>
</tr>
<tr>
<td>Cor Reinhard</td>
<td>Consultant PQR</td>
<td><a href="mailto:cri@pqr.nl">cri@pqr.nl</a></td>
<td>Reviewer</td>
<td>@CORequisITe</td>
</tr>
<tr>
<td>Frans Oudendorp</td>
<td>Consultant PQR</td>
<td><a href="mailto:fou@pqr.nl">fou@pqr.nl</a></td>
<td>Writer</td>
<td>@oudendorp</td>
</tr>
</tbody>
</table>

**Special thanks to:**

**Alistair Gillespie**, for reviewing the version 1.0 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.

**Kenny Buntinx** for reviewing the document and provide great feedback. Kenny is a highly qualified, certified managing consultant at KBsolutions with more than 15 years of experience. He has a strong focus on the Microsoft System Center product family and is an industry expert in the System Center Enterprise Client Management space. Additionally he believes strongly in sharing knowledge amongst his peers and therefore co-founded the System Center User Group Belgium (www.scug.be). As an industry expert and Most Valued Professional (MVP), he is a frequent speaker and ask-the-expert guest at both national and international events. To contact Kenny directly email or follow Kenny on twitter or look at his blog.

**Falko Gräve** for reviewing the document and provide great feedback and excellent help. He has been working as a Consultant and Architect at various IT services companies for more than 10 years. Falko now works in the global Hosted Desktop team at Evonik Industries in Germany. Besides technical certifications of desktop Virtualization products, Falko is an Most Valuable Professional (MVP) for Microsoft App-V. You can contact Falko via twitter or his blog.
3. ENTERPRISE MOBILITY

3.1 ENTERPRISE MOBILITY AS ONE OF THE TOP PRIORITIES

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 directly attached to the end-user, the business consumer, it is important to understand the role of ‘tomorrow’s datacenter’ and ‘tomorrow’s 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-X (Device, Screen, Location, OS, Application, Browser) Online/Offline, Managed/Un-Managed.
- 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” (http://en.wikipedia.org/wiki/Consumerization)

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 not 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, AnyBrowser, 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 abbreviation for one of the hottest trends. ‘Bring Your Own’, ‘Buy-Your Own’ ... in the grand scheme of solutions it is more about ‘Who owns the device’, what is the balance between self-reliant, freedom and control. Do you need control? If you need control, then 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 latest version can be found at:

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?
- Are there any legal aspects in your country that influence your decision?

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 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’.
3.3.1 Mobile Application Delivery

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

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

3.3.2 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

By using the Software Development Kit (SDK) from the MAM vendor it can be made sure that management features are hooked into 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 challenge with that is Digital Rights Management (DRM) and encryption, being 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.

3.3.3 HTML5 and (Mobile) Web Apps

Most of today’s corporate web-architected applications are not based on HTML5, they are 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 they are not designed and therefore not 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 meet 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. The browser on the mobile platform will limit HTML5 apps, 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 underlying mobile platform and other applications can be challenging.

3.3.4 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, trackpad, 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 IT as a Service and Tomorrows IT Organization

Business Consumers expect or demand solutions. If the IT organization does not fulfill demands, end-user will often go and find solutions elsewhere. ShadowIT or ‘StealthIT’ are the terms used to describe IT solutions used inside organizations without organizational approval. StealthIT solutions are often not in line with the organization’s requirements for control, security, reliability, documentation etc. To avoid 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.
3.5 Enterprise Mobility Management 2014 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 2014 Jack Madden updated his book Enterprise Mobility Management. In this book, Jack Madden digs into the rapidly-changing EMM field that has emerged in, what he calls, 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 that book for even more (background) information on the changes that Enterprise Mobility Management brings for users and companies. That book is a must read!
4. **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 fulfill the demands.

Before 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.

4.1 **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?

4.2 **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? Email, 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 Mobile IT strategy?
- What is the (business) applications **vendor support** policy for EMM?

4.3 **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?

4.4 **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?

4.5 **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?

4.6 **Generic**
- Who is the owner of the Mobile IT 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?
- Are 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.*
5. ENTERPRISE MOBILITY MANAGEMENT

5.1 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 email;
- Secure Data;
- Secure Web browsers.

5.2 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 to be ‘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 APIs. These APIs determine the capabilities of the MDM solution. If the mobile OS does not support a particular restriction (e.g. “block the camera”) an MDM product simply cannot enforce this restriction. Therefore, all MDM vendors have access to the same APIs provided by the OS and are theoretically able to deliver the exact same functionality on the management side.

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 APIs. 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! With the upcoming release of the future versions of Android, with additions like “Android for Work” (based on Samsung KNOX framework), things might get easier. Only time will tell.

As mentioned before, the MDM vendors provide largely the same features, as they are all dependent on the APIs 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 APIs 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!’.

Remember that MDM is just a tool that influences other characteristics like the User Experience, Policy Enforcements and others.

5.3 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 ap-
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 entire 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 3.3.2 for a short comparison 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 or sign applications. Whether you can use ‘app wrapping’ or an SDK is determined by the feature set of your MAM product AND it only works for that MAM product. Consider this when choosing your best solution!

5.4 **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. In fact you can use the previously discussed MAM to control information access on the application level. But that case the users are not free to choose whatever application they like to use. As MIM focuses on the data, regardless of the application, it probably would be the Best Fit to support Consumerization of IT.
However 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 starting with chapter 5.6.

5.5 **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.

5.6 **Secure Email**

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

Secure email 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 protect the corporate mail, calendar and contacts.

Probably the easiest (and most limited) method is using 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 are 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. This also differs from the various platforms; i.e. iOS 7 and above offers a ‘managed open in’ feature to prevent opening attachments in insecure apps.

The last method is to use a third-party email client such as Citrix WorxMail (iOS and Android), Airwatch Inbox, IBM MaaS360 Secure Productivity Suite, Nitrodesk Touchdown (iOS and Android) or Divide, recently purchased by Google. The email client is generally delivered using Mobile Application Management solutions 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 allowed to open attachments. Because the third-party email client is executed 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 email. A key question is – will users be willing to step away from the na-
ative app for their corporate mail and use a different and much more secure alternative email 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.

5.7 **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.

5.8 **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.
6. VENDORS AND THEIR EMM SOLUTIONS

6.1 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 vendors provide the vendor solution descriptions. However, we have attempted to remove the marketing fluff wherever possible.

6.2 AIRWATCH BY VMWARE

INTRODUCTION

Founded in 2003, AirWatch® by VMware® 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) support, multi-user management and much more. AirWatch employs over 1,800 people, with more than 600 in research and development – the largest in the EMM space. 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 12,000 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 nine global offices in Atlanta, Washington D.C., United Kingdom, Australia, India, Singapore and others.

VMware acquired AirWatch early 2014. This acquisition expands VMware's End-User Computing group; AirWatch offerings will form an expanded portfolio of mobile solutions that are complementary to VMware's portfolio.

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** - The AirWatch Mobile Device Management solution enables businesses to address challenges associated with the mobile devices by taking complex issues and creating simplified, comprehensive and user-friendly solutions without sacrificing security. Our solution 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 di-
verse fleet of Android, Apple iOS, BlackBerry, Mac OS, Symbian, Windows Mobile and Windows Phone devices from a single console.

- **Mobile Application Management** - The AirWatch Mobile Application Management solution 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. Install applications over-the-air with a customizable and brandable App Catalog, and ensure the right apps get to the right users with configurable user group requirements and assignments.

- **Mobile Content Management** - The AirWatch Mobile Content Management solution allows you to secure document distribution and mobile access to corporate documents through a native mobile app. AirWatch® Secure Content Locker™ enables your employees to securely access corporate resources on-the-go and collaborate on content from their Apple iOS, Android and Windows phones, tablets and PCs.

- **Mobile email Management** - AirWatch Mobile email Management integrates with your existing email infrastructure to deliver comprehensive security for monitoring access to your corporate email. With the AirWatch platform, you can enable secure mobile access to email, control mobile devices accessing email, prevent data loss, encrypt sensitive data and enforce advanced compliance policies.

- **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** - The AirWatch platform allows users to share devices without compromising security. To prevent unauthorized access, each user is authenticated before checking-out and using a device. Settings can be configured across an organizational group or specific to individual users. Shared devices remain enrolled and under management during the check-out and check-in process, so devices are always secure, even when not in use.
ARCHITECTURE

AirWatch scales to support deployments of thousands of devices through a robust architecture that is fully configurable according to customer environments and requirements. The AirWatch 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. Key features of AirWatch include:

- **Scalability** – Designed to easily support from 10 to over 100,000 devices supporting business growth over time. Reduces overall IT investments and achieves higher ROI by adding, editing and removing users and hardware when needed.

- **Multi-tenancy** – Enables device management based on user roles, device types or location groups. IT administrators can maintain control of the entire device fleet at a global level. Integrates with Active Directory and supports smart group creation.

- **Configurability** – Provides diverse options for customizing deployments to fit business needs. Enables businesses to control and change different aspects of their deployment to ensure optimal usage.

- **High Availability** – Supports using network load balancers, hypervisor technologies and server clustering to provide a highly available solution from the application servers to the SQL database.

- **Disaster Recovery** – Meets strict requirements for redundancy and disaster recovery through load balancing across multiple, geographically disparate data centers.

- **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, ensuring users receive appropriate profiles and access to apps and content.

- **Certificates and PKI** – Integrate to Microsoft CA, CA, or SCEP certificate services providers, such as MSCEP and VeriSign.

- **Email Infrastructure** – Manage and monitor mobile email through tight integration to your corporate 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 with automatic connections and centrally updated user credentials.

- **File Systems** – Integrate directly with existing file systems, including SharePoint, Google Drive, OneDrive, 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. For perpetual licenses, there is no yearly license cost other than a maintenance fee.

- Subscription License – Monthly fee per device, maintenance included
- Perpetual License – One-time fee per device, annual maintenance fee applies

Deployment Options

AirWatch provides two options for deploying their solutions – in the AirWatch Cloud or on-premise. 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

The AirWatch solution can be deployed, managed and maintained fully on-premise. Whether you are using dedicated hardware or virtualized environments, AirWatch delivers flexibility, scalability and control. On-premise customers benefit from full control over the management and maintenance of the system. Maintenance and system upgrade fees apply.

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
6.3 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 remote 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 email.** 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 email 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 either secure native email 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 direc-
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 email 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 email 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 make 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.

6.4 BlackBerry Enterprise Service 10 (BES10)

INTRODUCTION

Founded in 1984 as Research in Motion (RIM), BlackBerry revolutionized the enterprise mobility market with the 1999 introduction of the BlackBerry smartphone. Over the past 15 years, the company’s multi-platform enterprise mobility management (EMM) solution has amassed thousands of patents and dozens of industry certifications, qualifying it for inclusion in the networks of the world’s most security sensitive organizations, including the US Department of Defense (DoD). BlackBerry’s EMM footprint extends to more than 80,000 enterprises around the world. The BlackBerry Enterprise Service 10 (BES10) EMM has been installed on more than 30,000 test and commercial servers.

BlackBerry’s EMM platform is part of a layered, end-to-end solution that includes a secure network infrastructure and a mobile device operating system. The company is focused on four key mobile objectives: security, productivity, communications and collaboration. BlackBerry’s corporate headquarters are in Waterloo, Ontario, Canada. It also operates offices in North America, Europe, Asia Pacific and Latin America. The Company trades under the ticker symbols “BB” on the Toronto Stock Exchange and “BBRY” on the NASDAQ.
The BlackBerry Enterprise Mobility Management solution provides the following functions:

- **Mobile Device Management** - BES10 provides comprehensive management and security controls for corporate-issued and BYOD BlackBerry, iOS and Android devices, with support for MS Windows to be added in 2014. BES10 provides multi-platform device management capabilities through a simple administration console and, if required, extends security and control to the highest level. BlackBerry’s MDM offering supports self-service capabilities for basic management functions that helps to reduce helpdesk workload. BES10 is the evolution of BlackBerry Enterprise Server. It offers a natural upgrade to existing BES infrastructures, allowing enterprises to expand MDM capabilities to include support for BlackBerry 10, iOS and Android devices.

- **Mobile Application Management** - Mobile application management (MAM) is embedded into BlackBerry’s EMM solution, enabling IT departments to manage all aspects of the app lifecycle, including updating and retirement. BES10 can provision apps remotely over the air. Apps can be assigned to end users either from commercial stores or through the BlackBerry enterprise app store. Users are either prompted to install, receive silent install or select from an on-device app catalogue. Update notifications are sent automatically. Administrator controls include whitelists, mandatory install and update options, as well as options to control sharing data between apps, as well as authentication. BlackBerry provides containerization solutions that guard against data leakage and malicious attacks, while supplying end users with a near-native user experience. BlackBerry Balance enables BlackBerry 10 devices to be segregated into Work and Personal Spaces. BlackBerry extends the BES10 security and MAM capabilities to iOS and Android devices through BlackBerry Secure Work Space (SWS). Managed applications are secured and separated from personal apps and data, providing an integrated email, calendar and contacts app, an enterprise-level secure browser and secure attachment viewing and editing with Documents To Go. User authentication is required to access secure apps and work data cannot be shared outside the secure work space.

- **Mobile Content Management** - BlackBerry’s EMM solution offers extensive data and security management functions for BlackBerry, iOS and Android environments, including file sync & share, end-user or automated network drive & SharePoint mapping, offline file access, integration with cloud content providers and secure collaboration via Work Drives, Messenger and the Cloud File System on BlackBerry devices.

- **Mobile Security** - BlackBerry delivers protection for corporate content on device and in transit through comprehensive content and app security. Work content and apps are separated from personal content and apps while retaining the native user experience, with data leakage protection ensuring work information can’t be shared through personal channels. Complete app management and security means organizations can easily make work apps and content available to users across mobile platforms, as well as monitor and manage app usage and compliance from a single unified console. Seamlessly enabling secure access to systems behind the firewall, as well as protecting work data in transit, is assured by the proven BlackBerry security model, which now extends to multi-platform support. Simple setup and on-going administration is supported by BlackBerry’s VPN-less connectivity model – including certified end-to-end encryption. BlackBerry is one of the few enterprise mobility specialists to offer a layered security model, providing protection for the hardware, software and device OSs in its end-to-end solution. BES10 allows provisioning of certificates and supports SCEP-based provisioning. Certificates uses include ability to authenticate in the browser, messaging...
server, Wi-Fi network, VPN or for S/MIME. BlackBerry provides multiple identity and access options, depending on requirements of organization. The BlackBerry OS Crypto Kernel has FIPS 140-2 validation. The BlackBerry enterprise solution provides the security controls to comply with various requirements in regulations such as HIPPA/SOX, etc.

- **Mobile Application Development** - BlackBerry’s partnerships with leading enterprise software vendors and support for open-standards and open-source app development frameworks enables enterprises to efficiently and effectively mobilize and deploy business apps. A broad developer community and established development platform provides the support, tools and APIs to help enterprises build apps tightly integrated into the core features and management capabilities of the BES10 platform. BlackBerry’s mobile application development platform also assists businesses in maintaining the native experience users demand when deployed to iOS and Android devices through BlackBerry Secure Work Space.

- **Multiple Device Management Policies** - The BlackBerry end-to-end EMM solution supports the full spectrum of enterprise use cases and risk profiles. An organization’s device management policy requirements may vary from business unit to business unit or country to country. Organizations must also be able to manage devices based on employee role, security risk and compliance requirement, updating policies, for example, when an employee moves from an unregulated position to a regulated one. BlackBerry’s user-centric approach to EMM enables businesses to assign a variety of device management policies, including Corporate-Owned, Business-Only (COBO), Corporate-Owned, Business-Enabled (COPE) and BYOD, which can be administered from a single console and easily monitored and managed.
ARCHITECTURE

BES10 is available as an on-premise solution, as well as a hosted option. A market preview for multi-tenant cloud is also currently available. In February 2014, BlackBerry announced that the next version of BES would be commercially available before the end of the year and support a variety of deployment scenarios, including on-premise, public cloud, private cloud and hybrid environments.

BES10 can be installed on a single server and includes components for managing BlackBerry OS, BlackBerry 10, iOS and Android devices from a single platform and unified management console.

BES10 makes use of BlackBerry’s secure Infrastructure. A single outbound-initiated connection over port 3101 enables simplified installation and a secure behind-the-firewall connection for secured work applications on BB, iOS & Android devices.

A single BES10 server instance can currently manage up to 30K devices. Multiple server instances can be managed within a single domain (shared database). A single domain can manage up to 50K BB10 devices and 50K iOS and Android devices.

- **Email** - BES10 enables admins to configure ActiveSync email profiles that are securely deployed to end users upon device enrollment. ActiveSync protocol enables client mail support for a diverse set of on-premise and cloud-based email systems, including Exchange, Domino/Traveler, and Groupwise, as well as Office365 and Google Apps.

- **Directory Services** - BES10 integrates with Microsoft Active Directory as well as other LDAP-based directory systems to enable user creation, attribute and group synchronization, as well as administrator sign-on and end user authentication.

- **Reporting and Analytics** - The BES10 reporting solution offers a pre-configured, graphical system dashboard consisting of various charts that display critical system information. The reporting dashboard gives administrators a high-level overview of their BES10 environment. For example, you can view the number of devices in your organization by wireless service provider. You can drill down into a report to get additional...
details, export the information to a .csv file, view user details, and perform administrative tasks.
- **Web Services** - BlackBerry Web Services are a collection of SOAP web services that can be used to create applications to manage an organization's BES10 domain. They are used to automate many of the tasks that administrators typically perform using the administration consoles. For example, you can integrate user creation with existing tools for network account creation.

**LICENSING**

BlackBerry EMM capabilities extend across two levels to meet the needs of customers with varying device management, security and control requirements. The two licensing models, Silver and Gold, support both subscription and perpetual licensing models.

- **Silver level EMM** – Delivers multi-platform management and security for BlackBerry, iOS and Android smartphones and tablets – including comprehensive app management across all these platforms.
- **Gold level EMM** - Delivers security, control and app management of BlackBerry, iOS and Android smartphones and tablets for organizations that need the highest levels of security, require stringent and granular controls over device usage and will need to comply with strict security policies.

**6.5 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 Home.

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.
KEY FEATURES

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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure secure &amp; provision mobile devices</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>One-click live chat &amp; support</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Access SharePoint &amp; network drives</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Secure mobile web browser</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>App-specific micro VPN</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Secure mail, calendar and contacts app</td>
<td></td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>Enterprise-enable any mobile app</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Seamless Windows app integration</td>
<td></td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>Unified corporate app store</td>
<td></td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>Multi-factor single sign-on</td>
<td></td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>Secure document sharing, sync &amp; editing</td>
<td></td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>Both cloud &amp; on-premises data storage options</td>
<td></td>
<td>•</td>
<td>•</td>
</tr>
</tbody>
</table>

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 at least 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 config-
ure, securely distribute, and manage each prepared application by using App Controller.

- **Citrix Worx Home** is client software installed on the user device that allows users to access their apps and data through App Controller. Worx Home will also be used to enroll a device via Device Manager.

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 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.

### 6.6 **Cortado Corporate Server**

**INTRODUCTION**

Cortado – formerly ThinPrint – has delivered solutions for the modern working world since 1999. Enterprise Mobility, Printing and Virtualization are the focus business areas of the company. Cortado delivers productivity solutions which enable users to accomplish customary office work independent from device, location and system boundaries, alone and in teams. Easy for users, innovative and sustainable are the distinguishing qualities of Cortado products.

Cortado established itself internationally with ThinPrint, the leading printer virtualization technology, which is used in over 80 countries by thousands of companies. Even the biggest customers of Citrix XenApp and Microsoft Remote Desktop Services rely on ThinPrint. Via a long-term OEM partnership, VMware integrates ThinPrint technology.

Cortado, privately held and headquartered in Berlin, also has offices in USA, Australia, Japan, France and UK with about 250 employees.

Cortado Corporate Server is a complete Enterprise Mobility Solution that covers Mobile Device Management, Mobile Application Management and Mobile Content Management. It integrates seamlessly into the existing environment, as it is AD integrated and based on the existing Windows rights system. It enables customers to secure devices and content, manage corporate and in-house created applications and allows the users to be productive and flexible on any device, at anytime, anywhere.
ARCHITECTURE

Cortado Corporate Server is a client-server solution. The server component is installed in the backend behind the firewall and runs all clients. The Cortado client, tailored to the respective mobile platform, is installed on smartphones and tablets or is available as an HTML5 version on all other web-enabled mobile devices. The open architecture of Cortado Corporate Server is fully scalable and supports all common file formats. Compared to other cloud desktop or file sharing solutions, up to 90% less data is transferred due to intelligent compression and by carrying out data operations on the server-side. Several security layers protect content and backend access.

Customers can benefit from the ease and speed of new mobile devices on the one hand, as well as the performance and security of a centralized IT infrastructure on the other.

Mobile Device Management

Cortado Corporate Server comes with an HTML5 based Management Console. This console serves to create and roll-out MDM policies and is also the tool to configure the complete mobile environment. User groups are managed, network drives and printers assigned, user settings applied, productivity and security options selected, password policies set... it goes far beyond MDM and is basically a tool to seamlessly integrate mobile devices (including laptops, Macbooks...) into the existing Windows environment.

Mobile Device Management with Cortado Corporate Server:
- Secure and manage devices
- Roll-out policies
Mobile Application Management

MAM is also part of the Cortado Management Console. Via the apps tab in the control panel, admins can either import in-house apps or link to apps in the available app stores. App settings can be determined (is it a managed app, is it mandatory...). Based on the settings, apps are either pushed to the users devices or can be pulled from the enterprise app store that the users can find in their user portal. The administrator can remotely delete managed apps. By supporting the native app management on iOS and Samsung devices with Samsung managed apps, customers can build their own business app container without the need of app wrapping or using SDKs. Even virtual (Windows) apps are accessible via the Secure Browser called Secure Net.

Mobile Content Management

Cortado offers native applications for iOS, Android and BlackBerry (older version as they expect migration to other devices) that enable users to be productive by doing their office work on the go. They offer a file access and productivity client (Cortado Workplace) which is the client part of the Server-Client combination. The client allows access to the network shares on the file server and SharePoint. A second app, the secure browser named Cortado Net delivers access to intranet sites as well as virtual applications. This way, users get access to all the content they are working with. Files can be viewed, shared via email or link, edited, printed to network or wifi printers (on iOS even via the native print dialogue), transformed into other formats... basically, all typical file handling options that are needed to be productive and to work in a team are supported. For collaboration scenarios, the intelligent “Smart Filing” comes into play which facilitates the saving of files back onto the file server after editing or offline use, and it creates versions in case several users were working on one document at the same time.

Both apps are available for individual users as well (as Cortado Workplace with a Cloud storage instead of connection to the network shares and as Page2PDF, which can be used for PDF conversion of a website for offline use or reading). Cortado uses the feedback of their over 450,000 individual users to constantly improve the business apps.

The clients intelligently work with the Cortado server in the backend. Most file handling processes only take place in the backend, which saves a lot of bandwidth. One Cortado Corporate Server can carry up to 1000 users!

Cortado Corporate Server in a nutshell:
- Easy integration into the existing IT environment
- Native app management
- Vast offer of productivity and collaboration features
- Easy enrollment of devices
- All the needed MDM functionality
LICENSING

Cortado Corporate Server is available in a User-based licensing model (unlimited devices per user) in either an annual or a perpetual license.

6.7 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 secure access
- Provide two-factor authentication and S/MIME email signing and encryption
- 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
- 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 Enterprise**, for MDM, local data store, secure (intranet) browser and secure wireless email and PIM.
- **Good Dynamics**, for developing (SDK), securing and deploying containerized applications.
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 being/that are 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 consists 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 notification email 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). This allows 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** 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 enhanced data protection. User keys and credentials can be stored on smartcards and microSDs, so that the form factor of the mobile device and/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 reconfigurations, 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 an 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.

6.8 IBM MaaS360

IBM acquired Fiberlink and its award winning MaaS360 platform in December of 2013. MaaS360 is an Enterprise Mobility Management platform that allows companies to fully embrace mobile technology and quickly scale deployments throughout their organization. With MaaS360, businesses of any size can support the expanding need for employee productivi-
ty and privacy, security, and convenience enabled by bring your own device (BYOD) initiatives. MaaS360 provides a wide range of containerization options for mobile security that enable corporate and personal information to be separated. This gives customers the flexibility of tiered and layered mobile security to address their varied end-user needs and IT security requirements across users, devices, content and apps. MaaS360 is available in SaaS or on-premises deployment.

MaaS360 provides a range of product modules and bundles to enable customers to effectively meet their mobility requirements:

- 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.

**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. Content repositories such as SharePoint, NFS, Box, Google Drive. Robust sets 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.

Before an organization deploys third party applications, they must be contained and secured. A list of applications, which are certified and leverage advanced security policies directly though MaaS360, can be found on the MaaS360 Market web site.

MaaS360 Market Apps enable:

- Authentication and single sign-on
- Data leak prevention policies to restrict cut-copy-paste,
- Restrictions for “open-in” to whitelisted apps
- Block app usage for MDM policy non-compliance
- In-app VPN for corporate intranet access
- App data encryption

**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. In addition, users can also save, edit, and sync documents between all of their devices.

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, file shares, Box, Google Drive, 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 MaaS360 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. MaaS360 is also offered in an on-premises version.

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.

- **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). Perpetual licensing is also available.
6.9 **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 is 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 Microsoft Exchange Server. This protocol is primarily used for synchronization of email, contacts and calendaring tasks from the server to the device. When Microsoft enabled device synchronization in Exchange Server somewhere in 1996, no other use was needed but to synchronize email to devices. This was primarily because these devices where only able to synchronize email.

When the smartphones (and later on the tablets) arrived, it was possible to synchronize more than only email data and there for in an enterprise environment security of devices became more and more important.

Exchange ActiveSync still can do quite a lot in securing and controlling your mailbox data between the client and the device. However, Mobile Device Management features in Exchange ActiveSync are not as complete as a true MDM solution, but the enable you to:

- Limit reply/forward of corporate email
- Enforce the use of passwords when synchronizing from devices
- Allow, block or quarantine specific devices or device families
- Enable or disable the use of ActiveSync per user
- Control whether the download and opening of attachments is allowed or not
- Control whether a device needs to be encrypted or not
- Control if contacts can be synced to a device or not
- Since Exchange Server 2010 SP1 it is possible to elaborate the features available in Windows Right Management Services (RMS)*.
  - Perform a remote wipe
  - Number of failed logon attempts.

Microsoft Exchange ActiveSync provides the simplest protection for your mobile workforce. If you have an Exchange Server organization or Office 365 tenant and you want to synchronize email data, but have no additional need for MDM solution, using Exchange ActiveSync could be a solution to fulfill the need.

**LICENSING**

Exchange ActiveSync is part of the Microsoft Exchange Server and Client Access Licenses.

* Rights Management Services can help to encrypt and allow specific data and a form of selective functionality based on policies. RMS enables enterprises to secure confidential data like email, documents and corporate web pages.
6.10 **MICROSOFT ENTERPRISE MOBILITY SUITE**

**INTRODUCTION**

Microsoft Enterprise Mobility Suite is a combination of different products offered by Microsoft, and is part of their People Centric IT approach:

- Microsoft Windows Server Work folders
- Microsoft Workplace Join
- Microsoft Windows Server Web Application Proxy
- Microsoft Azure Active Directory
- Microsoft Azure Rights Managements
- Windows Intune

With Microsoft Enterprise Mobility Suite 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.x yet)
- Inventory hardware and software
- Upgrade to Windows 8.x Enterprise or run select prior Windows releases

**MICROSOFT WINDOWS SERVER WORK FOLDERS**

Microsoft Work Folders is a solution to access your personal data, which is stored on a file-server, from anywhere. Work Folders is a great solution for organizations who wants to store their data on their own file-servers. Work Folders include the following functionality:

- Provide a single point of access to work files on a user’s work and personal PCs and devices
- Access work files while offline and sync with the central file server the next time the PC or device has Internet or local network connectivity
- Maintain data encryption in transit as well as at rest on devices and allow corporate data wipe through device management services such as Windows Intune
- Use existing file server management technologies such as file classification and folder quotas to manage user data
- Specify security policies to instruct user PCs and devices to encrypt Work Folders and use a lock screen password, for example
- Use Failover Clustering with Work Folders to provide high-availability solution

How does Work Folders compare to other sync solutions that Microsoft provides, mainly OneDrive and OneDrive Pro? Work Folders is a solution for customers that prefer to use a Windows file servers as the backend storage for the corporate data.
**MICROSOFT WORKPLACE JOIN**

With Workplace Join it’s possible to register a non-domain joined device in Active Directory to get access to network resources. This is possible from many devices such as Windows 8 or Windows 7 but also IOS devices are supported.

Workplace Join is a lighter version of Domain Join, and is about authenticating an unknown device like a Surface RT, iOS or Android device. Workplace Join will put a certificate on the device, and can challenge the device for this as part of claims based authentication to applications or other resources such as data, plus there is no admin control of the device, it remains under the control of the end user.

When coupled with BYO device management with a solution like Windows Intune, you can apply policy, deploy apps and control access to resources on machines that you otherwise have no control over.

**MICROSOFT WINDOWS SERVER WEB APPLICATION PROXY**

Web Application Proxy is a new Remote Access role service in Windows Server 2012 R2. Web Application Proxy provides reverse proxy functionality for web applications inside your corporate network to allow users on any device to access them from outside the corporate network. Web Application Proxy pre-authenticates access to web applications using Active Directory Federation Services (AD FS), and functions as an AD FS proxy.

**MICROSOFT AZURE ACTIVE DIRECTORY**

Azure Active Directory is a service that provides identity and access management capabilities in the cloud. In much the same way that Active Directory is a service made available to customers through the Windows Server operating system for on-premises identity management. Azure Active Directory can be used as a standalone solution, but it can also be integrated with your on-premises Active Directory. When integrated with the on-premises Active Directory the directory sync technology is used to synchronize the objects. Applications such as Office365 and SharePoint can be integrated in Azure Active Directory to provide single-sign-on access.
**MICROSOFT AZURE RIGHTS MANAGEMENT**

Azure Rights Management can help to protect organization’s data from unauthorized access, and control how this information is used. Rights Management uses encryption, identity, and authorization policies to help secure your files and email. In comparison to standard access controls, such as NTFS permissions, protection that is applied by using Rights Management stays with the files and emails, independently of the location – inside or outside your organization, networks, file servers, and applications. You remain in control of your data even when it is shared with other people.

For example, you can configure a file so that only people in your organization can access it, or control whether the file can be edited, or restricted to read-only, or prevent it from being printed. You can configure emails similarly, and in addition, prevent them from being forwarded or prevent the use of the Reply All option. These protection tasks can be simplified and streamlined for your end users by using standardized policy templates.

Azure Rights Management is a cloud service, and is integrated into other Microsoft cloud services and applications for simple ease-of-use and persistent protection.

**WINDOWS INTUNE**

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 have support for this agent. Within the latest update Android support has been added aswell. Before, you needed to use System Center 2012 R2 Configuration Manager integration for that. In the same way this functionality can be offered on Windows, iOS and Android.

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

<table>
<thead>
<tr>
<th>Device</th>
<th>Operating System</th>
<th>Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Surface</td>
<td>Windows RT</td>
<td>Direct</td>
</tr>
<tr>
<td>Windows Phone 8</td>
<td>WP 8.0</td>
<td>Direct</td>
</tr>
<tr>
<td>Windows Phone 7</td>
<td>WP 7.x</td>
<td>EAS</td>
</tr>
<tr>
<td>iPad, iPhone, iPod Touch</td>
<td>iOS 4.0 or later</td>
<td>Direct</td>
</tr>
<tr>
<td>Android-based devices</td>
<td>Android 2.1 or later</td>
<td>Direct</td>
</tr>
<tr>
<td>Microsoft Surface Pro</td>
<td>Windows 8.x</td>
<td>Direct</td>
</tr>
<tr>
<td>PC devices</td>
<td>Windows XP SP3, Vista, 7, 8.x</td>
<td>Direct</td>
</tr>
</tbody>
</table>
With a new updates 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. For the next months Microsoft has announced to release multiple smaller updates to improve Intune’s usability. This is for both Intune standalone and with System Center 2012 R2 Configuration Manager integration.

**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 tasks are performed in SCCM entirely. To combine both products, SCCM 2012 with Service Pack 1 or R2 must be in place. EAS support is available for both solutions with an Exchange connector. With the SCCM connector in place there is support for up to 100,000 computers.

**CLOUD-BASED MANAGEMENT (WINDOWS INTUNE STANDALONE)**

- No existing Configuration Manager deployment
- Simplified policy control
- Less than 7,000 devices and 4,000 users
- Simple web-based administration console

![Figure 1: Windows Intune](image.png)
UNIFIED DEVICE MANAGEMENT (WINDOWS INTUNE WITH SYSTEM CENTER)

- Build on existing Configuration Manager deployment
- Full PC management (OS Deployment, Endpoint Protection, application delivery control, rich reporting
  - Requires Full Configuration Manager client!
- Deep policy control requirements
- Scale to 100,000 devices
- Extensible administration tools (RBA, PowerShell, SQL Reporting Services)

Figure 2: Windows Intune with System Center Configuration Manager

INTUNE CONSOLE

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 performing/executing daily management. In this console (which is based on Microsoft Silverlight) user/device groups, software updates, endpoint protection, software packages, and policies are managed. As the Admin console is a web based application, it can be used from anywhere.
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 email.
- **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. In that scenario the native management console is obsolete. Remember, once Intune is connected to SCCM and it takes ownerships, there is NO way back.

**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 to 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 to users (optional installation) or to devices (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. The current 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 applied to 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.

### 6.11 MobileIron

**Introduction**

MobileIron is a purpose-built Mobile IT platform for enterprises to secure and manage mobile applications, content, and devices while providing their employees with device choice, privacy, and a native user experience. MobileIron’s competitive advantages are depth of data security and app management, rich ecosystem of best-of-breed third-party apps, track record of innovation, and focus on customer success. MobileIron also has one of the highest employee satisfaction scores in the industry (glassdoor.com). On June 12, 2014, MobileIron became a publicly-traded company on the NASDAQ stock exchange.

MobileIron’s vision is that mobility unlocks human potential in the workplace. The MobileIron solution 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, content, and web. These services are directly accessed by end users from their devices/. MobileIron provides delivery, configuration, and data-at-rest protection for these services, along with ongoing posture and compliance checking.
  - Apps@Work is for distributing apps through an enterprise app store
  - Docs@Work is for mobile content management
  - Web@Work is for secure mobile browsing
  - AppConnect is the client-side containerization capability (SDK and wrapper) for securing data-at-rest for mobile application management
  - Help@Work is for remote access and troubleshooting
  - Tunnel is for per-app VPN
  - Dataview is for monitoring mobile data usage for expense management
- **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, content, and web. The MobileIron Sentry can be installed as either a physical or virtual appliance.

- Tunnel is the per-app VPN implementation of Sentry

**Policy and configuration engine** to ensure mobile apps, docs, and devices can be managed end-to-end at global scale.

- The engine is called MobileIron Core for on-premises deployment and MobileIron Cloud for cloud deployment.
- MobileIron Insight is a tablet app for on-the-go EMM so that administrators can manage their mobile deployments when they are, themselves, mobile
- MobileIron App Delivery Network provides highly scalable, global distribution of in-house apps

The MobileIron solution can be deployed in three ways:

- On-premise as either a hardened virtual or physical Linux appliance, which lowers total cost of ownership over Windows-based EMM solutions
- Public cloud as the multi-tenant MobileIron Cloud service hosted by MobileIron.
- Private cloud hosted by MobileIron partners globally

**MobileIron: Purpose-built architecture**

**INNOVATION**

MobileIron has a track record of innovation in EMM and has been granted eight patents to date:

- Management of mobile applications (enterprise app store) – Jan 2013, May 2014
- Selective management of mobile device data in an enterprise environment (BYOD privacy policy) – Apr 2014
- Management of certificates for mobile devices (identity) – Jul 2013
- Mobile activity intelligence (usage/expense management) – Dec 2012
- Virtual instance architecture for mobile device management systems (3 patents) – Nov 2011, Mar 2013, Jan 2014
Customers - MobileIron has sold its solutions to over 6,000 customers worldwide. MobileIron is a true enterprise platform, with the majority of its business coming from enterprises with over 1,000 employees. MobileIron revenues in 2013 exceeded 100 million US dollars, with 56% coming from North America and 44% coming from outside North America.

Ecosystem - MobileIron works with more than 130 AppConnect partners and more than 36 Technology Alliance partners who have integrated, or are in the process of integrating, with the platform. MobileIron customers have used AppConnect to secure over 1,000 internally developed applications.

Customer Success - MobileIron’s global Customer Success team has developed the depth and breadth of expertise to provide customers with the support required on their journey to become Mobile First. In 2013, MobileIron’s renewal rate was greater than 90% for software support agreements and subscription licenses.

LICENSING

The core product licensing of MobileIron is per device or per user. Customers can choose a perpetual license or per month subscription licensing model. Support is included when choosing a subscription license, while with the perpetual license support is bought at an extra annual fee. MobileIron sells its products as a Silver, Gold, or Platinum bundle.

6.12 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. SMMS 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. SMSS 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** - SMSS 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 email Access** - SMSS 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** - SMSS provides a simple and secure user experience via strong authentication methods. SMSS supports authentication requirements on email, Wi-Fi and VPN, and integrates with Symantec Managed PKI Service and Microsoft Certificate Authorities. SMSS provides integrated single sign-on functionality across in-house and third-party apps, leveraging popular authentication methods including LDAP, SAML and SiteMinder. In addition, SMSS extends single sign-on to cloud apps through integration with the Symantec O3 web gateway.

- **Device Management** - SMSS provides comprehensive mobile device management capabilities providing visibility and control over smartphones and tablets. SMSS enables devices to access key corporate assets, such as email, calendar, critical mobile applications, documents, and media content. SMSS 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** - SMSS 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 wiped remotely.

- **Threat Protection** - SMSS 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** - SMSS 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. Symantec 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 APIs. 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.

### 6.13 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 for 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 VM, 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:

<table>
<thead>
<tr>
<th>Bundle or Suite</th>
<th>Components</th>
<th>Type of License</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizon View</td>
<td>Horizon View</td>
<td>Concurrent User</td>
</tr>
<tr>
<td></td>
<td>ThinApp</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Workstation *</td>
<td></td>
</tr>
<tr>
<td></td>
<td>vSphere Desktop</td>
<td></td>
</tr>
<tr>
<td></td>
<td>vCenter Desktop</td>
<td></td>
</tr>
<tr>
<td>Horizon Mirage</td>
<td>Horizon Mirage</td>
<td>Named User</td>
</tr>
<tr>
<td></td>
<td>ThinApp</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Workstation *</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fusion Pro</td>
<td></td>
</tr>
<tr>
<td>Horizon Workspace</td>
<td>Horizon Workspace</td>
<td>Named User</td>
</tr>
<tr>
<td></td>
<td>ThinApp</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Workstation *</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Horizon Mobile for Android</td>
<td></td>
</tr>
<tr>
<td>Horizon Suite</td>
<td>All three smaller bundles:</td>
<td>Named User or Concurrent</td>
</tr>
<tr>
<td></td>
<td>Horizon View</td>
<td>User</td>
</tr>
<tr>
<td></td>
<td>Horizon Mirage</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Horizon Workspace</td>
<td></td>
</tr>
<tr>
<td></td>
<td>vCenter Operations Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td>for View</td>
<td></td>
</tr>
</tbody>
</table>

* 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.
7. EMM FEATURES COMPARISON

7.1 INTRODUCTION

It is important to understand that comparing product features is the last step in the Mobile IT 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 are looking for. Keep the strategic questions mentioned in chapter 4 Mobile IT Strategy in mind!

Below you will find an overview of the various vendors, their solutions and the functionality they are offering at a very high level. We have 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.
7.2 **COMPARISON 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 7.6 – Compare Matrix, Features.

<table>
<thead>
<tr>
<th>MEM</th>
<th>AirWatch by VMware</th>
<th>Appense EMM Suite</th>
<th>Citrix XenMobile</th>
<th>Cortado Corporate Server</th>
<th>Good for Enterprise</th>
<th>IBM MaaS360</th>
<th>Microsoft Enterprise Mobility Suite</th>
<th>MobileIron</th>
<th>Symantec MM Suite</th>
<th>VMware Horizon</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile Device Management</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Mobile Application Management</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Mobile Information Management</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Mobile Expense Management</td>
<td>●</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td></td>
</tr>
<tr>
<td>Secure Mail Client</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Secure Data,FileSync</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Secure Web Browser</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
</tbody>
</table>

7.3 **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 an email to Peter Sterk (pst@pqr.nl).
7.4 **PRODUCT VERSION**

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

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Product</strong></td>
<td><strong>Version</strong></td>
<td><strong>Release date</strong></td>
</tr>
<tr>
<td>AirWatch by VMware</td>
<td>7.2</td>
<td>June 2014</td>
</tr>
<tr>
<td>Citrix XenMobile</td>
<td>9.0</td>
<td>June 2014</td>
</tr>
<tr>
<td>Good for Enterprise</td>
<td>2.4.0</td>
<td>June 2013</td>
</tr>
<tr>
<td>IBM MaaS360</td>
<td>n/a</td>
<td>June 2014</td>
</tr>
<tr>
<td>Microsoft Enterprise Mobility Suite</td>
<td>On-going</td>
<td></td>
</tr>
<tr>
<td>MobileIron</td>
<td>7.0</td>
<td>June 2014</td>
</tr>
</tbody>
</table>

7.5 **FEATURE COMPARE MATRIX**

<table>
<thead>
<tr>
<th>EMM solutions and features</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Goal:</strong></td>
<td>Detailed description of features</td>
</tr>
<tr>
<td><strong>Requirements:</strong></td>
<td>Hands-on-experience, vendor involvement</td>
</tr>
<tr>
<td><strong>Result:</strong></td>
<td>Whitepaper</td>
</tr>
<tr>
<td><strong>Method of Execution:</strong></td>
<td>Hands-on experience, read articles, communicate with vendors and discuss with colleagues</td>
</tr>
</tbody>
</table>

**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 is out of scope for this whitepaper to explain the ‘It depends’ remarks.”
## 7.6 Compare Matrix, Features

<table>
<thead>
<tr>
<th>Category</th>
<th>AirWatch by VMware</th>
<th>Citrix XenMobile</th>
<th>Good for Enterprise</th>
<th>IBM MaaS360</th>
<th>Microsoft EMS</th>
<th>MobileIron</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported (mobile) platforms</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Android 2.2</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>~</td>
<td>✓</td>
<td>EMS: only in combination with EAS</td>
</tr>
<tr>
<td>Android 3.x</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>~</td>
<td>✓</td>
<td>EMS: only in combination with EAS</td>
</tr>
<tr>
<td>Android 4.x</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Android 4.x, support for Samsung KNOX</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Android 4.x, support for Samsung SAFE</td>
<td>✓</td>
<td>✓</td>
<td>#</td>
<td>✓</td>
<td>#</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Apple iOS 4.x</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Apple iOS 5.x</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Apple iOS 6.x</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Apple iOS 7.x</td>
<td>✓</td>
<td>✓</td>
<td>#</td>
<td>✓</td>
<td>#</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Apple TV</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>#</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Apple MAC OS X</td>
<td>✓</td>
<td>~</td>
<td>X</td>
<td>✓</td>
<td>~</td>
<td>✓</td>
<td>~EMS: With SCCM FULL client only</td>
</tr>
<tr>
<td>BlackBerry 7.x</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>BlackBerry 10</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Linux</td>
<td>X</td>
<td>~</td>
<td>X</td>
<td>~</td>
<td>X</td>
<td>✓</td>
<td>~EMS: With SCCM FULL client only</td>
</tr>
<tr>
<td>Symbian</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>EMS: With SCCM FULL client only</td>
</tr>
<tr>
<td>Category</td>
<td>AirWatch by VMware</td>
<td>Citrix XenMobile</td>
<td>Good for Enterprise</td>
<td>IBM MaaS360</td>
<td>MobileIron</td>
<td>Remarks</td>
<td></td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------------------</td>
<td>------------------</td>
<td>---------------------</td>
<td>-------------</td>
<td>------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>Windows Mobile 6.x</td>
<td>✓ ✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Phone 7.5</td>
<td>✓ ✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Phone 8.x</td>
<td>✓ ✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows XP SP3</td>
<td>✓ ✓ X ✓ ✓ X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows 7</td>
<td>✓ X X ✓ ✓ X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows 8.x</td>
<td>✓ ✓ X ✓ ✓ ✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows RT</td>
<td>✓ ✓ X ✓ ✓ ✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iOS - Supports Apple MDM device management APIs</td>
<td>✓ ✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WP8 – Supports Exchange Active Sync management policies</td>
<td>✓ ✓ # ✓ ✓ ✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Mobile Device Management – (not all features are supported on all Mobile Platforms)**

<table>
<thead>
<tr>
<th>Feature</th>
<th>AirWatch by VMware</th>
<th>Citrix XenMobile</th>
<th>Good for Enterprise</th>
<th>IBM MaaS360</th>
<th>MobileIron</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block noncompliant OS platforms and versions</td>
<td>✓ ✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Block noncompliant applications</td>
<td>✓ ✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restrict access from noncompliant devices,</td>
<td>✓ ✓ ✓ ✓ ✓ X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Max number of devices per user, for instance 5.</td>
<td>✓ ✓ ✓ ✓ ✓ X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application whitelisting</td>
<td>✓ ✓ # ✓ ✓ ~</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application blacklisting</td>
<td>✓ ✓ ~ ✓ ✓ ~</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Send alerts for policy violations</td>
<td>✓ ✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enforce password complexity</td>
<td>✓ ✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Category

<table>
<thead>
<tr>
<th>Category</th>
<th>AirWatch by VMware</th>
<th>Citrix XenMobile</th>
<th>Good for Enterprise</th>
<th>IBM MaaS360</th>
<th>Microsoft EMS</th>
<th>MobileIron</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enforce password duration</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Enforce password expiration</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Enforce password lock after time of inactivity</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>EMS: Intune standalone only</td>
</tr>
<tr>
<td>Remote lock</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>EMS: Intune standalone only</td>
</tr>
<tr>
<td>Remote wipe - full</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>EMS: With SCCM integration only</td>
</tr>
<tr>
<td>Remote wipe – selective</td>
<td></td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>EMS: With SCCM integration only</td>
</tr>
<tr>
<td>Certificate-based authentication</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>X</td>
<td>√</td>
<td>√</td>
<td>MobileIron was granted the patent for mobile certificate management in July 2013 (<a href="https://www.google.com/patents/US8494485">https://www.google.com/patents/US8494485</a>)</td>
</tr>
<tr>
<td>Certificate distribution</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>X</td>
<td>√</td>
<td>√</td>
<td>EMS: With SCCM integration only</td>
</tr>
<tr>
<td>Certificate revocation</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>X</td>
<td>√</td>
<td>√</td>
<td>EMS: With SCCM integration only</td>
</tr>
<tr>
<td>Manage firewall on device, if applicable</td>
<td>X</td>
<td>√</td>
<td>X</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>Windows Mobile &amp; Android only</td>
</tr>
<tr>
<td>Manage antivirus on device, if applicable</td>
<td>~</td>
<td>X</td>
<td>~</td>
<td>√</td>
<td>√</td>
<td>~</td>
<td>~ iOS only</td>
</tr>
<tr>
<td>Manage VPN on device, if applicable</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>~</td>
<td>√</td>
<td>~</td>
<td>EOS: Intune with SCCM integration only</td>
</tr>
<tr>
<td>Monitor, audit and report message flows</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>X</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Application Inventory</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>AirWatch by VMware</td>
<td>Citrix XenMobile</td>
<td>Good for Enterprise</td>
<td>IBM MaaS360</td>
<td>Microsoft EMS</td>
<td>MobileIron</td>
<td>Remarks</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>---------------------</td>
<td>------------------</td>
<td>---------------------</td>
<td>-------------</td>
<td>---------------</td>
<td>------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Application distribution through enterprise app store</td>
<td>✓ ✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>MobileIron was granted the patent on MAM (enterprise app store) in January 2013 (<a href="https://www.google.com/patents/US8359016">https://www.google.com/patents/US8359016</a>)</td>
</tr>
<tr>
<td>Integration with Apple Volume Purchase Program</td>
<td>✓ ✓ ✓ ✓ x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integration with Google Playstore volume licensing</td>
<td>x x x x x x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Not available/supported by Google today</td>
</tr>
<tr>
<td>Over-the-Air updates for applications</td>
<td>✓ ✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Over-the-Air updates for mobile OS</td>
<td>~ ~ ~ ~ ~ ~</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>~ Windows Mobile only</td>
</tr>
<tr>
<td>Support for Role Based Access Administration</td>
<td>✓ ✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit logging available in management console</td>
<td>✓ ✓ x ✓ x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Block external memory in mobile devices, if applicable</td>
<td>✓ ✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure wireless networks on the device</td>
<td>✓ ✓ ~ ~ ~ ~</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>~ iOS &amp; Windows Mobile only</td>
</tr>
<tr>
<td>Limit wireless networks on the device</td>
<td>~ ~ ~ ~ ~ ~</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>~ Android only</td>
</tr>
<tr>
<td>Prevent screen captures for specific apps or data</td>
<td>✓ ✓ x ✓ x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>~ EMS: Intune with SCCM integration only</td>
</tr>
<tr>
<td>Locate devices</td>
<td>✓ ✓ x ✓ x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Schedule deployments to devices</td>
<td>✓ ✓ x ✓ ✓ ✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>~ Windows Mobile only</td>
</tr>
<tr>
<td>Specify conditions for deployments to devices</td>
<td>✓ ✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>AirWatch by VMware</td>
<td>Citrix XenMobile</td>
<td>Good for Enterprise</td>
<td>IBM MaaS360</td>
<td>Microsoft EMS</td>
<td>MobileIron</td>
<td>Remarks</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------</td>
<td>------------------</td>
<td>---------------------</td>
<td>-------------</td>
<td>---------------</td>
<td>------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Inventory carrier network</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>~</td>
<td>√</td>
<td>~ iOS only</td>
</tr>
<tr>
<td>Inventory mobile country code</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>~</td>
<td>√</td>
<td>~</td>
<td>~ iOS only</td>
</tr>
<tr>
<td>Inventory network code</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>~</td>
<td>√</td>
<td>~</td>
<td>~ iOS only</td>
</tr>
<tr>
<td>Android – Detect rooted devices</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enroll devices in bulk</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td>X</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Enroll devices by user</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Enroll devices by email</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Enroll devices through native app</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>√</td>
<td>EMS: only on iOS and Android</td>
</tr>
<tr>
<td>Shared device management / multi-user</td>
<td># # # # # # #</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile Application Management – (not all features are supported on all Mobile Platforms)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deploy Android Apps</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Deploy Android Google Playstore apps</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deploy Apple Apps</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Deploy Apple App Store Apps</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Deploy MAC OS X Apps</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>X</td>
<td>X</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Deploy Windows Apps</td>
<td>√</td>
<td>√</td>
<td>X</td>
<td>√</td>
<td>√</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Deploy Windows Store Apps</td>
<td>√</td>
<td>√</td>
<td>X</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Deliver Windows Apps</td>
<td>√</td>
<td>√</td>
<td>X</td>
<td>√</td>
<td>√</td>
<td>~</td>
<td>EMS: Intune</td>
</tr>
<tr>
<td>Category</td>
<td>AirWatch by VMware</td>
<td>Citrix XenMobile</td>
<td>Good for Enterprise</td>
<td>IBM Mac5930</td>
<td>Microsoft EMS</td>
<td>MobileIron</td>
<td>Remarks</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>--------------------</td>
<td>------------------</td>
<td>--------------------</td>
<td>-------------</td>
<td>---------------</td>
<td>------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Deliver Windows Phone Store apps</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Requires additional products from the vendor, like VMware Horizon, Citrix XenDesktop/XenApp</td>
</tr>
<tr>
<td>Push mandatory apps to devices</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>EMS: not all platforms</td>
</tr>
<tr>
<td>Create categories of apps</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Create list of suggested apps</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Support for third-party application stores</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Application wrapping</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>Deploy managed apps in one container</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>NO ONE can do this on iOS because Apple prohibits the download of executable code into an existing app on the device. Fundamental prohibition of iOS.</td>
</tr>
<tr>
<td>Deploy managed apps in different containers</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>Encryption of containers</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>Prevent data leakage to unmanaged apps</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>~</td>
<td>EMS: Azure Rights Managements</td>
</tr>
<tr>
<td>Control data exchange between managed apps</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>~</td>
<td></td>
</tr>
<tr>
<td>Verify application origin</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>Only true if supported by Mobile Operation System</td>
</tr>
<tr>
<td>Single Sign On for managed applications</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Application policies</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>AirWatch by VMware</td>
<td>Citrix XenMobile</td>
<td>Good for Enterprise</td>
<td>IBM MaaS360</td>
<td>Microsoft EMS</td>
<td>MobileIron</td>
<td>Remarks</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>--------------------</td>
<td>------------------</td>
<td>--------------------</td>
<td>------------</td>
<td>--------------</td>
<td>-----------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>- Set minimum mobile OS platform version for apps</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>- Set maximum mobile OS platform version for apps</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>- Exclude devices from specific apps</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>- Require logon on application start</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>- Require explicit logon on application start</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>- Require WiFi on application start</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>- Require network on application start</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>- Require device passcode</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>- Block jailbroken or rooted devices</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>Intune: Retire/Wipe</td>
</tr>
<tr>
<td>Android - Application whitelisting</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Android - Application blacklisting</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>iOS - Application whitelisting</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>iOS - Application blacklisting</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>WP8.x - Application whitelisting</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>WP8.x - Application blacklisting</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

**Mobile Information Management – (not all features are supported on all Mobile Platforms)**

<p>| Manage personal data on corporate device                                 | ✓                  | X                | ✓                  | ✓          | ✓            | ✓         | MobileIron was granted the patent for selective |
| Manage corporate data on personal device                                 | ✓                  | ✓                | ✓                  | ✓          | ✓            | ✓         |                                             |</p>
<table>
<thead>
<tr>
<th>Category</th>
<th>AirWatch by VMware</th>
<th>Citrix XenMobile</th>
<th>Good for Enterprise</th>
<th>IBM Mac5360</th>
<th>Microsoft EMD</th>
<th>MobileIron</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wipe personal data from corporate device</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Through full device wipe</td>
</tr>
<tr>
<td>Wipe corporate data on personal device</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Prevent data leakage to unmanaged apps</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>☒</td>
<td>✓</td>
<td>☒</td>
<td></td>
</tr>
<tr>
<td>Control data exchange between managed apps</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>☒</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Encrypt local data</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>☒</td>
<td>✓</td>
<td>☒</td>
<td>Only true if supported by Mobile Operating System</td>
</tr>
<tr>
<td>Allow access to information based on location</td>
<td>✓</td>
<td>✓</td>
<td>☒</td>
<td>✓</td>
<td>☒</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Distribute content to mobile devices</td>
<td>✓</td>
<td>☒</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Think of Enterprise file sync solutions</td>
</tr>
<tr>
<td>Distribute content to mobile devices with third-party apps</td>
<td>✓</td>
<td>☒</td>
<td>✓</td>
<td>☒</td>
<td>✓</td>
<td>✓</td>
<td>e.g. Accellion</td>
</tr>
<tr>
<td>Distribute content to mobile devices using encryption</td>
<td>✓</td>
<td>✓</td>
<td>☒</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Distribute content to mobile devices with third-party apps using encryption</td>
<td>✓</td>
<td>☒</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Send alerts for policy violations</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Block cut/copy/paste between personal and corporate apps</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>☒</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Secure access to on-premises webservises</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>☒</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Secure access to on-premises Microsoft Sharepoint</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Secure access to on-premises network shares</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>EMS: Workfolders</td>
</tr>
<tr>
<td>Android – media encryption</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>AirWatch by VMware</td>
<td>Citrix XenMobile</td>
<td>Good for Enterprise</td>
<td>IBM MaaS360</td>
<td>Microsoft EMS</td>
<td>MobileIron</td>
<td>Remarks</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>--------------------</td>
<td>------------------</td>
<td>---------------------</td>
<td>-------------</td>
<td>---------------</td>
<td>------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>Distribute Adobe PDF files to device</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Distribute image files to device (PNG, BMP, JPEG)</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Distribute Microsoft Office files to device</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Check if file exist, otherwise copy the file</td>
<td>✓</td>
<td>~</td>
<td>X</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Configure attributes for the file (readonly, hidden)</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Provide description for the file</td>
<td>✓</td>
<td>~</td>
<td>X</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>X ~ Android and Windows Mobile only</td>
</tr>
<tr>
<td>Specify destination location for the file</td>
<td>~</td>
<td>~</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X ~ Android and Windows Mobile only</td>
</tr>
<tr>
<td>Block Cloud services (e.g. iCloud)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>Only true if supported by Mobile Operation System</td>
</tr>
<tr>
<td>Monitor roaming usage</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Limit roaming usage</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>Only true if supported by Mobile Operation System</td>
</tr>
<tr>
<td>Prevent roaming usage</td>
<td>✓</td>
<td>~</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Only true if supported by Mobile Operation System</td>
</tr>
<tr>
<td>Send alerts for policy violations</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Secure email – (not all features are supported on all Mobile Platforms)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supports native app</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>With third party app</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Mailapp for Android is part of the solution</td>
<td>~</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>~ AirWatch Inbox requires Orange license or higher Android Email+ Divide is optional</td>
</tr>
<tr>
<td>Mobile Expense Management – (not all features are supported on all Mobile Platforms)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supports native app</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>With third party app</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>AirWatch by VMware</td>
<td>Citrix XenMobile</td>
<td>Good for Enterprise</td>
<td>IBM MaaS360</td>
<td>Microsoft EMS</td>
<td>MobileIron</td>
<td>Remarks</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>--------------------</td>
<td>------------------</td>
<td>---------------------</td>
<td>-------------</td>
<td>---------------</td>
<td>-----------</td>
<td>--------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Mailapp for iOS is part of the solution</td>
<td>~</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>~</td>
<td>~</td>
<td>~ Airwatch Inbox requires additional license ~ MobileIron: Divide is optionally available through MobileIron</td>
</tr>
<tr>
<td>Mailapp for Windows Phone 8.x is part of the solution</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Encrypt attachments</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Block specific attachments</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Support Exchange Active Sync device access rules</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Containerization of email profiles native mail client</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Containerization of email profiles with third-party mail client</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Prevent email forwarding based on content</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Prevent email forwarding based on attachments</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Prevent email forwarding based on user or user group</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Prevent email forwarding based on device or device group</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Configure email profiles on the device</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Microsoft Exchange Server 2010 support</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Microsoft Exchange Server 2013 support</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>AirWatch by VMware</td>
<td>Citrix XenMobile</td>
<td>Good for Enterprise</td>
<td>IBM MaaS360</td>
<td>Microsoft EMS</td>
<td>MobileIron</td>
<td>Remarks</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>--------------------</td>
<td>------------------</td>
<td>--------------------</td>
<td>-------------</td>
<td>---------------</td>
<td>------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Microsoft Office 365 support</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Google Gmail support</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>IBM Lotus Notes/Domino support</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>IMAP support</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Share (specific) details of corporate contacts with personal contacts</td>
<td>~</td>
<td>~</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>Export corporate to personal contacts</td>
</tr>
<tr>
<td>Support for FIPS 140-2 encryption</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td><strong>Platform/infrastructure</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud (SaaS) service available</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>On-premises solution, agents connect through outbound connection to a Cloud service</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>Good Technology uses a Network Operations Center running in the Cloud</td>
</tr>
<tr>
<td>Integration with Microsoft System Center 2012</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>High available deployment possible</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>~ No need for on-premises server</td>
</tr>
<tr>
<td>Disaster recovery techniques available</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>~ No need for on-premises server</td>
</tr>
<tr>
<td>Support for over 5,000 devices</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>~ Microsoft use ‘Users’, not devices</td>
</tr>
<tr>
<td>Support for over 10,000 devices</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>~ Microsoft use ‘Users’, not devices</td>
</tr>
<tr>
<td>Support for over 20,000 devices</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>~ Microsoft use ‘Users’, not devices</td>
</tr>
<tr>
<td>Active Directory supported</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>Citrix XenMobile</td>
<td>Good for Enterprise</td>
<td>IBM MaaS360</td>
<td>Microsoft EMS</td>
<td>MobileIron</td>
<td>Remarks</td>
<td></td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------------------</td>
<td>---------------------</td>
<td>-------------</td>
<td>---------------</td>
<td>------------</td>
<td>-----------------------------------</td>
<td></td>
</tr>
<tr>
<td>LDAP supported</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>No need for on-premises server</td>
<td></td>
</tr>
<tr>
<td>Windows Server 2003 support</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Available as a virtual appliance</td>
<td></td>
</tr>
<tr>
<td>Windows Server 2008 support</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>No need for on-premises server</td>
<td></td>
</tr>
<tr>
<td>Windows Server 2008 R2 support</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Available as a virtual appliance</td>
<td></td>
</tr>
<tr>
<td>Windows Server 2012 support</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>No need for on-premises server</td>
<td></td>
</tr>
<tr>
<td>Windows Server 2012 R2 support</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>Available as a virtual appliance</td>
<td></td>
</tr>
<tr>
<td>Support for two-factor auth</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>XY available as a virtual appliance</td>
<td></td>
</tr>
<tr>
<td>Support for multi-factor auth</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>XY available as a virtual appliance</td>
<td></td>
</tr>
<tr>
<td>Licensing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Licensed per user</td>
<td>X</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Licensed per device</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subscription license</td>
<td>✓</td>
<td>✓</td>
<td>~</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Perpetual license</td>
<td>✓</td>
<td>✓</td>
<td>~</td>
<td>✓</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## EMM Smackdown

<table>
<thead>
<tr>
<th>Category</th>
<th>AirWatch by VMware</th>
<th>Citrix XenMobile</th>
<th>Good for Enterprise</th>
<th>IBM MaaS360</th>
<th>Microsoft EMS</th>
<th>MobileIron</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>First year support and maintenance included in license</td>
<td>√</td>
<td>×</td>
<td>√</td>
<td>√</td>
<td>×</td>
<td>√</td>
<td>~ Main. and basic support included for subscription</td>
</tr>
<tr>
<td>Software Maintenance is mandatory for 1st year</td>
<td>√</td>
<td>√</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>√</td>
<td>~ Available option</td>
</tr>
<tr>
<td>24 x 7 support included in license</td>
<td>~</td>
<td>~</td>
<td>×</td>
<td>X</td>
<td>X</td>
<td>√</td>
<td>~ Windows Mobile only</td>
</tr>
<tr>
<td>Grace period</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>~ Available option</td>
</tr>
<tr>
<td>Free for personal usage (FFPU)</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>~ Available option</td>
</tr>
<tr>
<td>Free trial period</td>
<td>√</td>
<td>√</td>
<td>#</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>~ Available option</td>
</tr>
<tr>
<td>Free for students at educational institutions</td>
<td>X</td>
<td>#</td>
<td>#</td>
<td>#</td>
<td>#</td>
<td>#</td>
<td>~ Available option</td>
</tr>
<tr>
<td>Open Mobile Alliance device management v1.2 supported</td>
<td>√</td>
<td>×</td>
<td>×</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>~ Windows Mobile only</td>
</tr>
<tr>
<td>Granular network access control by integrating Cisco ISE 1.2</td>
<td>√</td>
<td>√</td>
<td>#</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>~ Windows Mobile only</td>
</tr>
</tbody>
</table>

### Support and Community

<p>| Certification program for ISVs                                        | X                  | √                | X                   | √           | X             | √          |
| Community forum available for public                                 | X                  | √                | X                   | √           | X             | X          |
| Community forum available for customers                              | √                  | √                | √                   | √           | X             | √          |
| Official training classes available                                  | √                  | √                | X                   | X           | √             | X          |
| Official certification program, VUE or Prometric                      | 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             | √          |</p>
<table>
<thead>
<tr>
<th>Category</th>
<th>AirWatch by VMware</th>
<th>Citrix XenMobile</th>
<th>Good for Enterprise</th>
<th>IBM MaaS360</th>
<th>Microsoft EMS</th>
<th>MobileIron</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>10+ of public available enterprise (10K CCU) references in EU using EMM technology stack</td>
<td>~</td>
<td>X</td>
<td>X</td>
<td>~</td>
<td>X</td>
<td>✓</td>
<td>MobileIron: only available for customers and partners</td>
</tr>
<tr>
<td>10+ of public available enterprise (10K CCU) references in US using EMM technology stack</td>
<td>~</td>
<td>X</td>
<td>X</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>MobileIron: only available for customers and partners</td>
</tr>
<tr>
<td>Vendor created reference design for enterprise architecture, public available</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>~</td>
<td>✓</td>
<td>~</td>
<td>MobileIron: only available for customers and partners</td>
</tr>
<tr>
<td>SMB Reference Architecture, public available</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>~</td>
<td>✓</td>
<td>~</td>
<td>MobileIron: only available for customers and partners</td>
</tr>
</tbody>
</table>
8. CHANGE LOG

DATE JULY 2014; DOCUMENT VERSION 2.0

- Added Cortado Corporate Server to chapter 6.6
- Updates to chapter 6.8 ‘IBM MaaS360’
- Added IBM MaaS360 to chapter 7.6 Compare Matrix, Features
- Removed AppSense EMM Suite from chapter 7.6 Compare Matrix, Features
- Removed Symantec EMM Suite from chapter 7.6 Compare Matrix, Features
- Removed chapter ‘Security’
- Removed chapter ‘Application and Desktop Delivery Solutions 3.0’
- Removed ‘Cisco Meraki’ from ‘Vendors and their EMM Solutions’
- Added ‘BlackBerry Enterprise Service’ to ‘Vendors and their EMM Solutions’
- Citrix XenMobile 9.0 release
- Windows Intune 5.0 update (Wave E) release
- Added license change to Horizon Suite in chapter 6.13
- Changed AirWatch text in chapter Error! Reference source not found. (acquisition by VMware).
- Changed AirWatch EMM Suite to AirWatch by VMware in document
- Changed AirWatch version and release date to 7.2 June 2014 in chapter 7.1
- Made numerous changes to AirWatch by VMware solution offerings in chapter 7.6
- Made numerous changes to MobileIron solution offerings in chapter 7.6
- Made numerous changes to Citrix XenMobile solution offerings in chapter 7.6
- Added Microsoft Enterprise Mobility Suite as chapter 6.10

DATE SEPTEMBER 2013; DOCUMENT VERSION 1.2

- Added note about IOS7 in chapter 7.3.
- Added feature ‘Secure access to on-premises network shares’, in table in chapter 9.5.
- Added feature ‘Granular network access control by integrating Cisco ISE 1.2’, in table in chapter 9.5.
- Change mobile client platform support “Windows XP Sp3”, “Windows 7” for AirWatch Enterprise Mobility Management Suite
- Change mobile client platform support “Windows 7”, “Windows 8” for Citrix XenMobile
- Added / changed description of Microsoft Exchange Active Sync
- Next release Windows Intune announced (Wave E)
- Architecture “Cloud-based and Unified Device Management”

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 😊
9. 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. Marcel can be reached at mkl@pqr.nl.

**Anton van Pelt** (1984) is a Technical Consultant at PQR. Antonhis 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 ape@pqr.nl.

**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 Microsoft Certified Systems Engineer (MCSE) and a VMware Certified Professional (VCP). Sven is also a Citrix Certified Enterprise Administrator (CCEA) and 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 he 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.
Frans Oudendorp (1981) works as a consultant at PQR. He started his IT career in 2002 as a system engineer and has grown into an all-round consultant. The focus of Frans is on Microsoft Private Cloud solutions. In particular, the new Microsoft People Centric IT solution has his attention. In addition, he has knowledge of the entire stack of Microsoft Private Cloud solutions such as Microsoft Hyper-V and all the System Center products. Frans has besides the Microsoft certification levels as Microsoft IT Professional (MCITP), Microsoft Certified Technology Professional (MCTS) and Microsoft Certified Solution Expert “Private Cloud” (MCSE Private Cloud) also other certification levels such as VMware Certified Professional (VCP) and Citrix Certified Administrator (CCA). You can reach Frans at fou@pqr.nl or twitter.