G00265601

Critical Capabilities for Enterprise Mobility Management Suites

Published: 9 June 2015

Analyst(s): Terrence Cosgrove, Rob Smith, Chris Silva, John Girard, Bryan Taylor

EMM products have become more complete, the market has become more competitive and the value of mobility is increasing. Mobility enables IT leaders to better engage with their customers, improve business processes and enable new business opportunities, so the selection of EMM vendors is critical.

Key Findings

- Enterprise mobility managers are using enterprise mobility management suites to support a broad range of device platforms, including iOS, Android, Windows Phone, Windows 8.1 and Mac OSX.
- Enterprise mobility managers are enabling a wide range of mobile use cases; 40% of the EMM Magic Quadrant and Critical Capabilities references stated that they were supporting a vertical industry or line-of-business use case (e.g., email and calendaring) beyond general productivity.
- The use of advanced features of EMM suites is growing, which increases the complexity of users' requirements.

Recommendations

- Identify the mobile use cases in your organization, and evaluate the EMM functions that are most critical in addressing those use cases.
- Identify the critical mobile applications for your organization, and select vendors that work best with those applications.

What You Need to Know

The value of mobility is extensive for most organizations. Mobility can enable organizations to better engage with customers, improve business processes and enable new business opportunities. However, mobile expansion cannot occur without operational integrity and reliability, which is

achieved, in part, through the use of enterprise mobility management (EMM) suites. Thus, EMM adoption continues to grow, driven by increased adoption across organizations through the general productivity use case — email, personal information manager (PIM), browsing, access to documents — as well as by functional and use-case expansion within organizations.

Generally more advanced than the overall industry, customer references for this report (n = 120) illustrate expanded EMM use. Forty percent were using their EMM tools for vertical use cases beyond basic productivity, 30% were supporting shared devices and 19% were using their EMM tools to support contactors using personal devices.

As use cases have expanded, so too has mobile application use and, often, the diversity of mobile platforms:

- Fifty-nine percent of the references reported that they use their EMM tools to manage internally-developed applications.
- Fifty-six percent stated that they use EMM to manage apps received from third parties and delivered through internal app stores.
- Fifty-eight percent were supporting public app store apps.

Apple iOS has been the dominant mobile platform in the enterprise for the past several years; 87% of references were supporting iOS. This year, references also reported substantial support for consumer Android (75%) and Windows Phone (37%).

Increased use of mobile applications and platforms drives increased use of EMM features. Mobile device management (MDM) provides the foundational capabilities, and 87% of references stated that they use the MDM features of their EMM product. Other features were widely used as well:

- The increased use of mobile applications has expanded the adoption of mobile application management (MAM); 31% stated that they use app wrapping, while 23% use MAM software development kits (SDKs).
- Secure PIM, which is often used when implementing bring your own device (BYOD) programs or supporting Android, saw 34% adoption among the references.
- Thirty-two percent of organizations surveyed were using the mobile content management (MCM) features of their EMM products.
- Finally, references also reported substantial use of EMM to manage certificates (beyond email) that improve security and usability for Wi-Fi (49%) and virtual private networks (VPNs; 35%).

These facts demonstrate the increased sophistication of EMM deployments. Organizations must consider a variety of factors when making an EMM vendor decision:

- The mobile use cases in the organization — e.g., general productivity, BYOD, line-of-business (LOB) applications
- Which applications and devices the organization must support to enable the mobile use cases
- Which advanced EMM functions will be required to enable the use cases

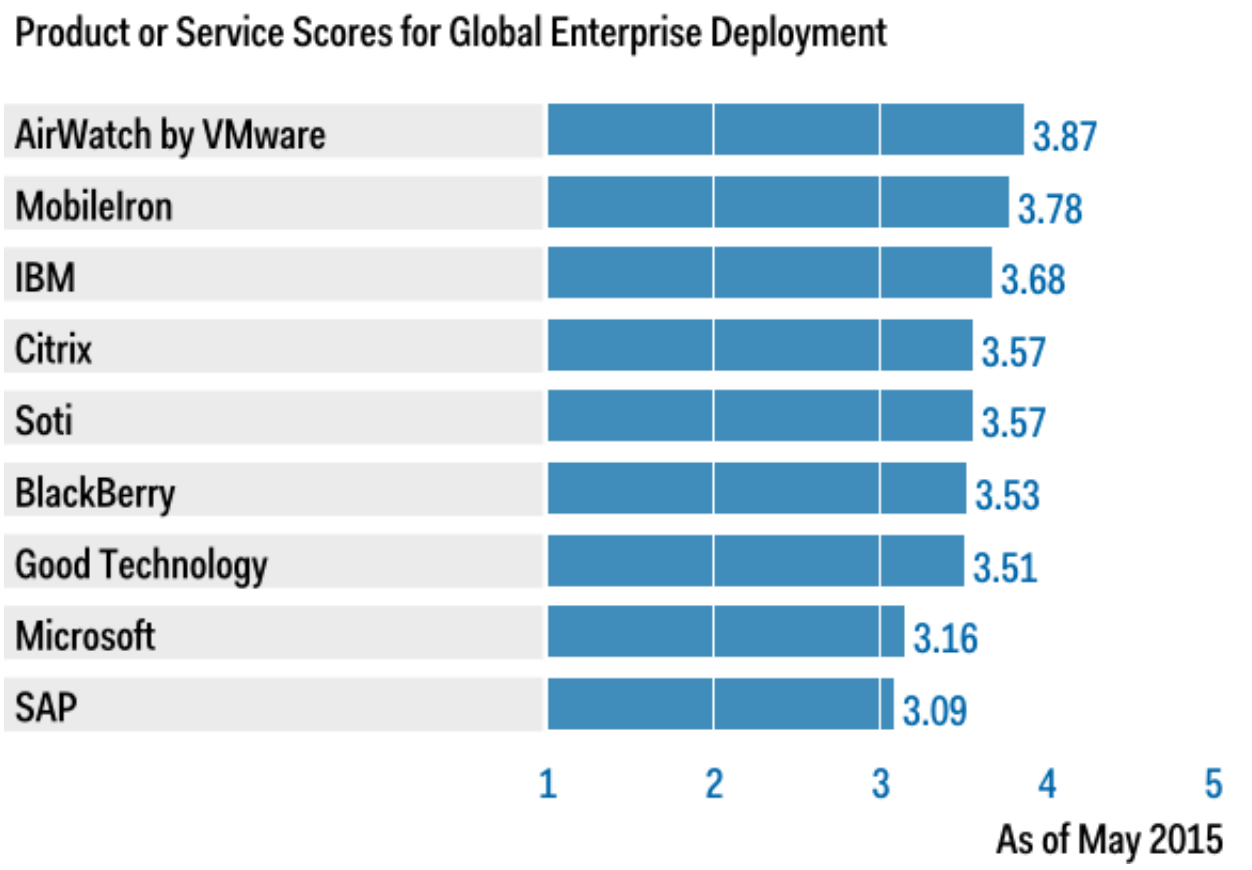
- Which EMM vendors work best with your organization's IT infrastructure
- The vendor's track record in keeping up with mobile OS changes and other customer requirements
- Overall vendor viability

Use the findings in this Critical Capabilities research to determine which vendors are best-suited to your particular use cases.

Analysis

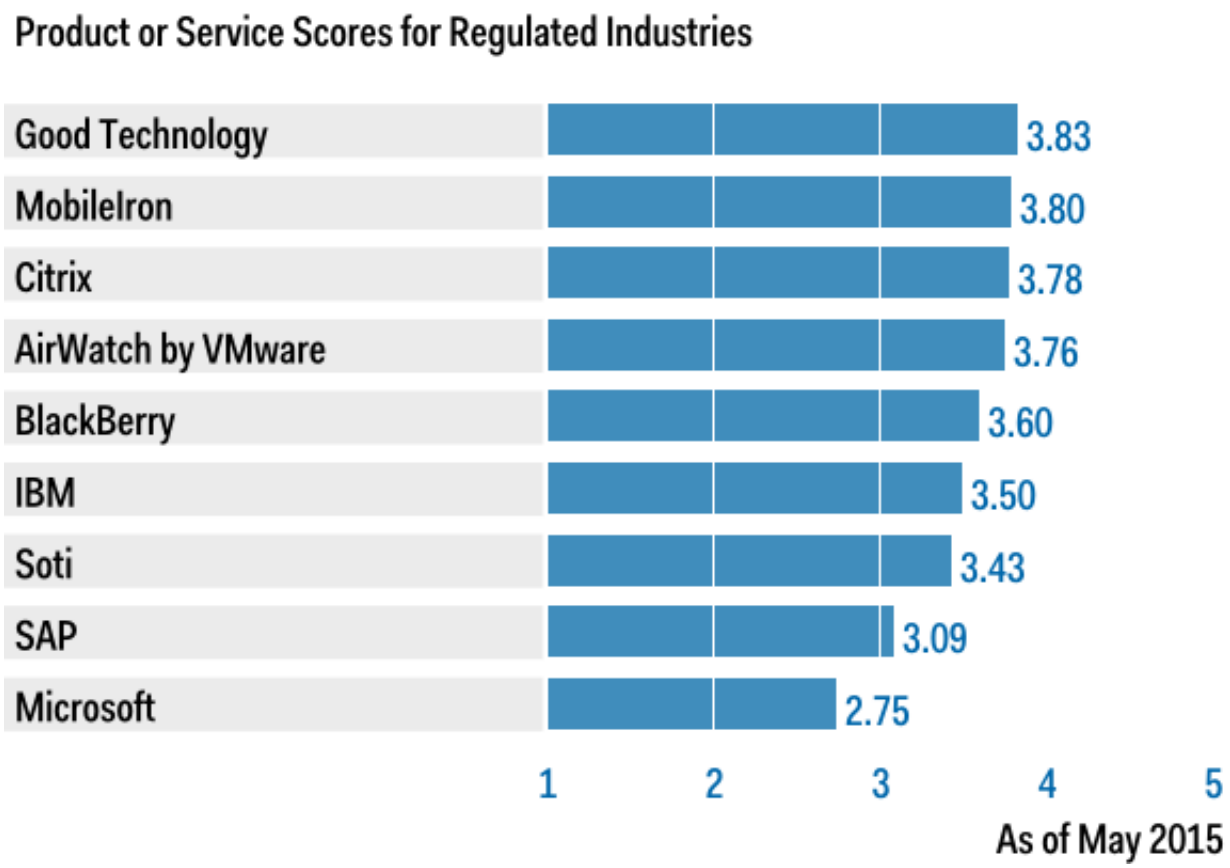
Critical Capabilities Use-Case Graphics

Figure 1. Vendors' Product Scores for the Global Enterprise Deployment Use Case



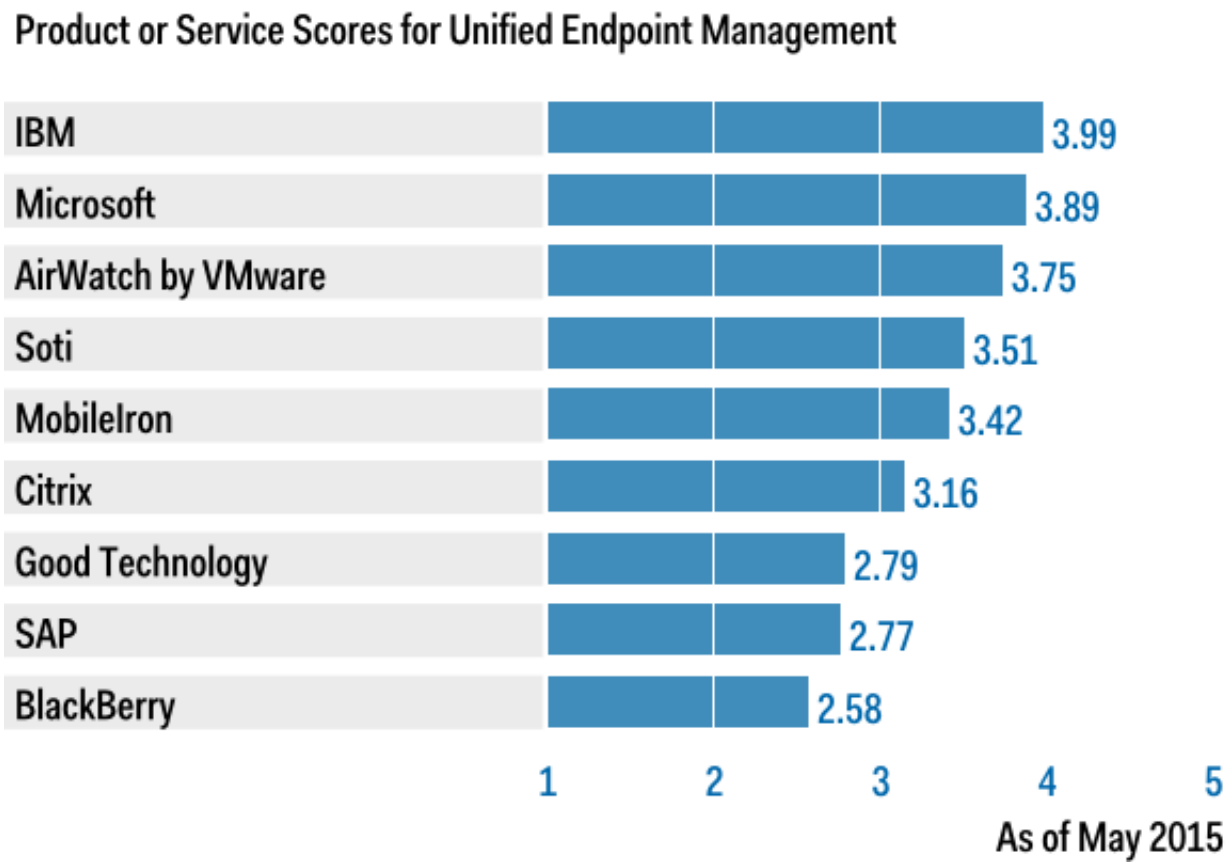
Source: Gartner (June 2015)

Figure 2. Vendors' Product Scores for the Regulated Industries Use Case



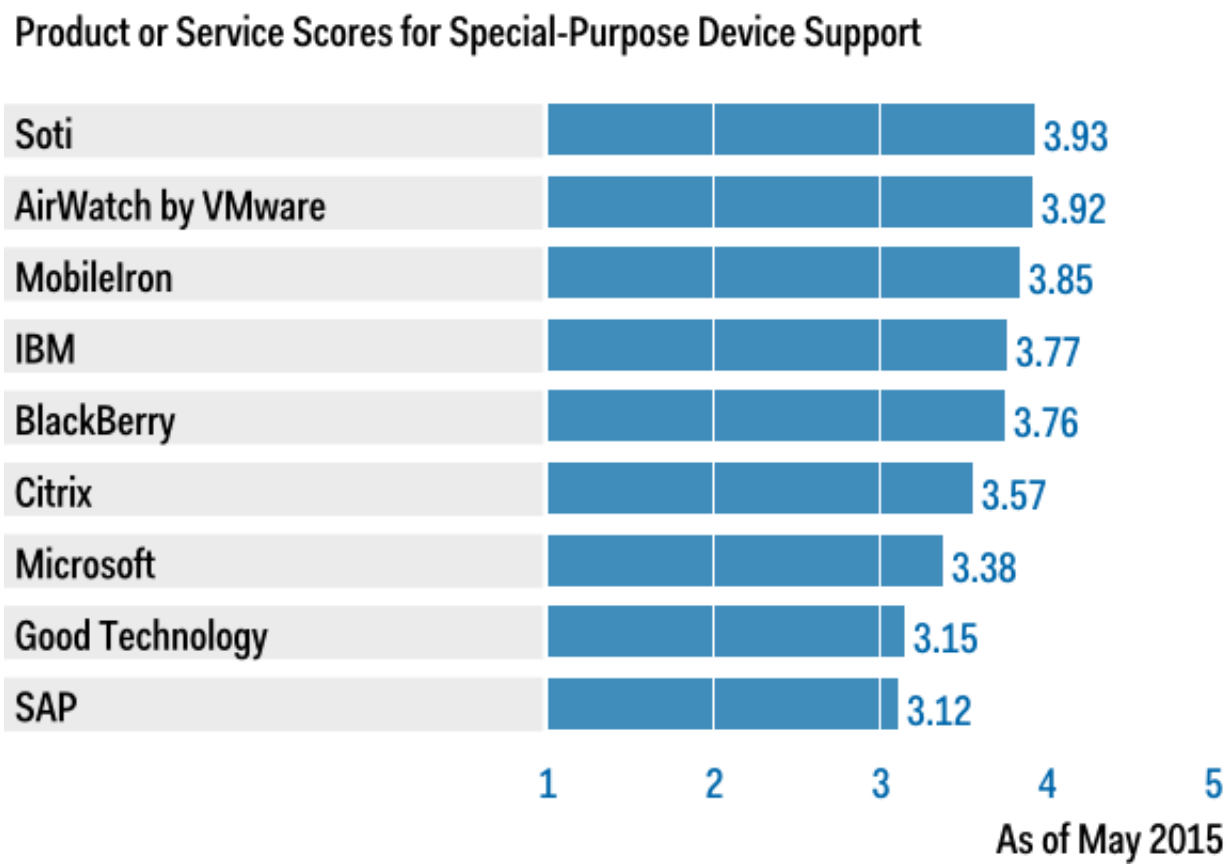
Source: Gartner (June 2015)

Figure 3. Vendors' Product Scores for the Unified Endpoint Management Use Case



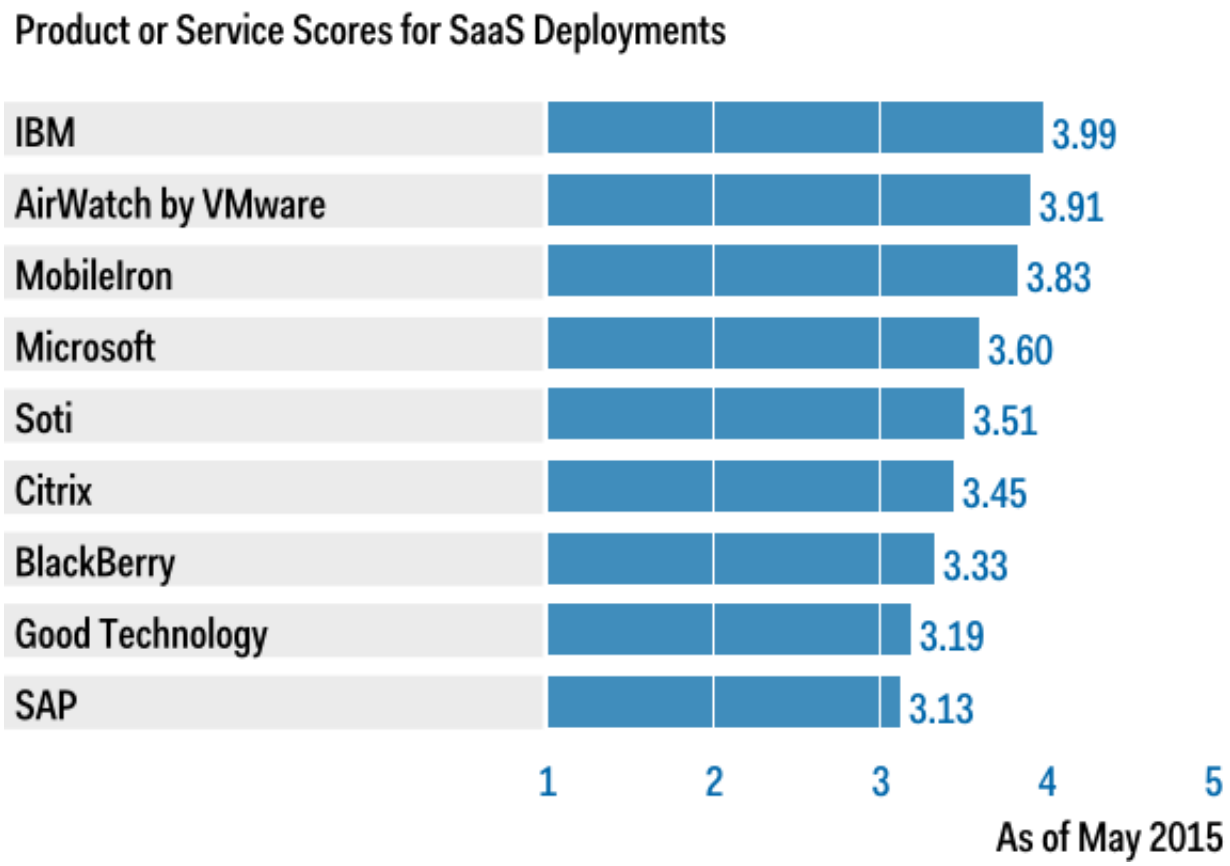
Source: Gartner (June 2015)

Figure 4. Vendors' Product Scores for the Special-Purpose Device Support Use Case



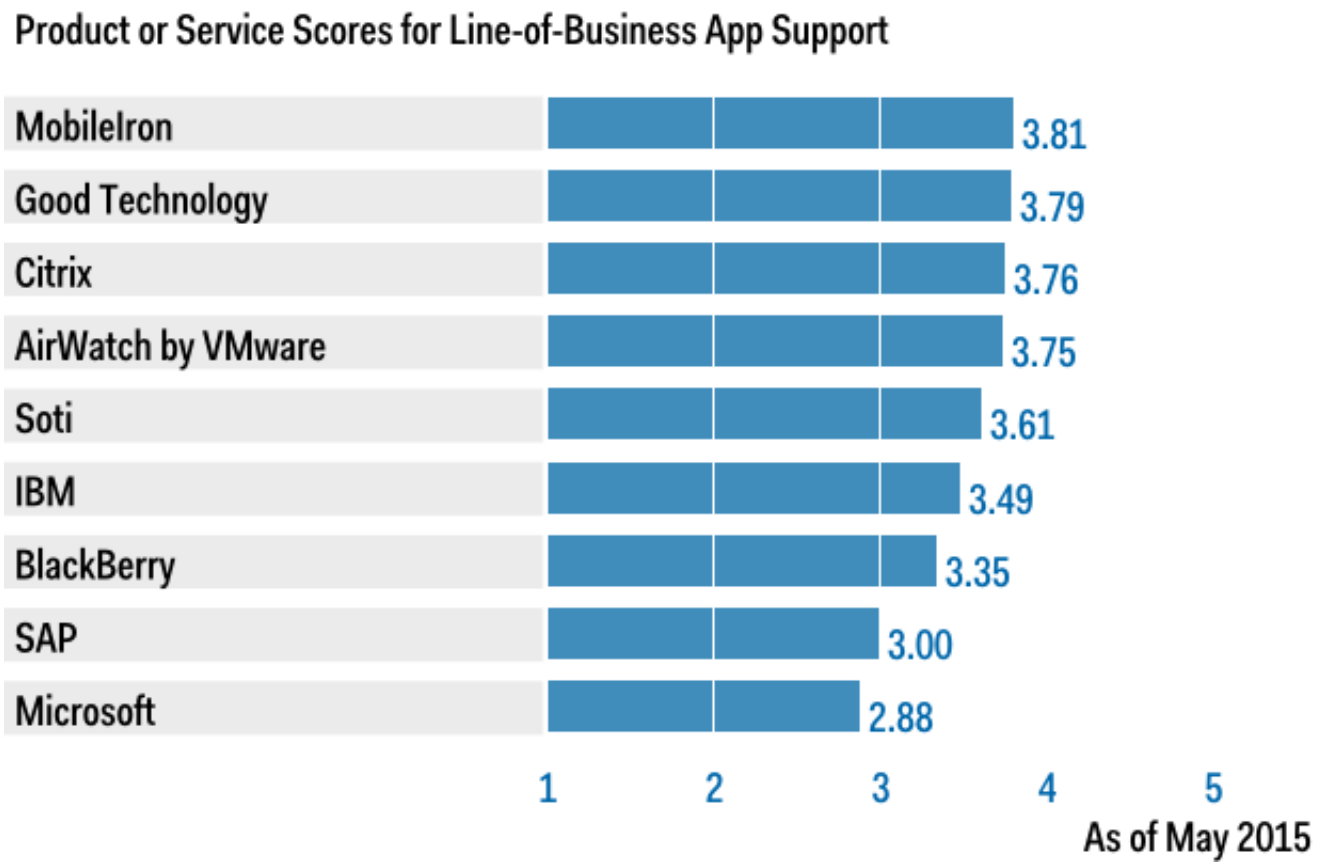
Source: Gartner (June 2015)

Figure 5. Vendors' Product Scores for the SaaS Deployments Use Case



Source: Gartner (June 2015)

Figure 6. Vendors' Product Scores for the Line-of-Business App Support Use Case



Source: Gartner (June 2015)

Vendors

AirWatch by VMware

AirWatch is one of the most functionally complete EMM offerings in the market. The AirWatch product is broad and targets every major mobile use case:

- AirWatch provides an excellent administrator user experience, with an intuitive interface, vertical-specific administrative templates and "getting started wizards" to bring administrators up to speed.
- AirWatch is excellent at creating policies based on a wide variety of criteria, and it provides a way to test the impact of MDM profiles before deployment.
- AirWatch scales well, and a large number of references have been managing more than 10,000 users in production.
- AirWatch supports a wide range of Android handset MDM APIs (e.g., LG and HTC); this is especially useful for special-purpose device scenarios.

- On-premises infrastructure components are based on Windows, SQL Server and Linux (not appliance-based), which adds administrative overhead, compared with many other on-premises products.
- AirWatch Inbox has improved during the past year; however, organizations continue to report stability issues. Gartner commonly sees organizations limit their use of Inbox to Android devices.
- Code quality, particularly with new releases, is an occasional issue with AirWatch. Gartner clients have reported several recent issues on both the console and the agent side.

BlackBerry

BlackBerry released BlackBerry Enterprise Service (BES) 12 in the fourth quarter of 2014. BES12 provides improved non-BlackBerry OS support, and it consolidates the management of BlackBerry devices, which previously required separate versions of BES, depending on the type of device:

- The BES12 console provides good navigation. The "filter grid" and "quick filters" make it easy to find users and devices, based on many attributes. It provides easy filtering and subfiltering.
- BlackBerry enables administrators to control which hardware models can run the BlackBerry Workspace (i.e., MAM). BlackBerry also updates the device whitelist/blacklist for customers, through the use of its network operations center (NOC). Administrators can control access to mobile applications and specific hardware devices by using hardware identifiers, such as the International Mobile Station Equipment Identity (IMEI) number.
- The NOC architecture has many benefits, including scalability and ease of installation without opening up ports.
- Administrators can address privacy issues by giving the user a MAM-only workspace. In our study of the product, there was no ability to set MDM-based privacy groups (e.g., block location tracking or disable device wipe), as is common in other EMM products.
- Although BES12 has a MAM module, it provides only app wrapping. Security and analytics capabilities are limited and inconsistent across platforms.
- Secure PIM on iOS and Android does not support certificates, and customers have reported usability problems, particularly on Android.
- BES12 does not support Windows 8.1 or Mac OSX.

Citrix

Citrix released XenMobile 10 in the second quarter of 2015. XenMobile 10 brought together the previously separate MAM and MDM consoles. For customers interested in XenMobile's full EMM capabilities, there are separate consoles for ShareFile and NetScaler for setup and administration:

- The XenMobile 10 console is intuitive, and it provides convenient ways for administrators to take action directly from the home page dashboard.

- MDX, which is Citrix's app-wrapping technology, and WorxMail, which is Citrix's Secure PIM, are promising capabilities that provide unique security functionality. The Worx apps, which are prebuilt and provided by Citrix, create a container with built-in workflows for common tasks, such as note taking and joining a Web conference.
- ShareFile is one of the best MCM products among the EMM vendors. It provides full enterprise file synchronization and sharing (EFSS) capabilities, and it's built to work with the broader Citrix container.
- The SaaS platform is a dedicated instance model. Citrix intends to provide a multitenant SaaS platform in the future.
- Gartner found XenMobile's ability to create device-based groups to be limited, relative to other EMM products.
- Mobile application configuration for the Worx apps is cumbersome, and they are difficult to administer at large scale.

Good Technology

Good released a major new version of its Good Secure Mobility Solution in 2014. This new version integrates Good Work, the Good Dynamics Platform and its MDM module:

- Good excels at MAM-oriented functions. Its MAM module enables organizations to embed services (e.g., presence and instant messaging), as well as advanced security functions (e.g., secure data sharing) into mobile applications that are a part of the Good Dynamics framework.
- Good enables administrators to control which hardware models can run the Good-secured applications. Good also updates the device whitelist/blacklist for customers through the use of its NOC. Administrators can control access to mobile applications to specific hardware devices by using hardware identifiers, such as IMEI number.
- A new function, called the "Good Launcher," provides a persistent icon and a simple interface that enable users to switch easily between apps.
- Good provides mobile application performance monitoring and analytics capabilities that are unique in the EMM market.
- Customers have reported numerous end-user functional limitations with the Good Work platform. Many of Good's 2015 updates are focused on addressing the feature parity gap between Good for Enterprise and Good Work.
- The administration of the Good environment needs improvement. There is a lack of integration among some of the products, and customers have reported that it's difficult to maintain an accurate count of active applications.
- Good's device management capabilities are not as strong as those of other leading products in administration, as well as the support of device-level functions.

IBM

IBM recently renamed its MaaS360 to MobileFirst Protect:

- IBM's MobileFirst Protect has a robust SaaS platform and a great deal of experience providing SaaS services.
- MobileFirst Protect's origins (Fiberlink) are in laptop management; it has agent-based and MDM support for Windows and Mac OSX devices.
- The product provides integrated anti-malware as a standard offering, using IBM Trusteer technology.
- MobileFirst Protect has many capabilities for controlling access to enterprise applications. In addition to integrating with VPN and network access control (NAC) vendors, MobileFirst Protect integrates with IBM ISAM to control access to mobile and Web apps based on location, IP address and reputation score. The product integrates with IBM QRadar to determine the reputation of a device or user that can be fed into a real-time access decision. QRadar can detect compliance events and then tell MobileFirst Protect to take action.
- The console's features include an activity feed, which shows recent events and can create customized alerts. However, we continue to get feedback from customers about console and administration issues. For example, records of retired devices remain in the system for a period of time, and there are sometimes issues synchronizing data between the mobile gateway and the MobileFirst Protect console.
- Based on our research, MAM (e.g., app wrapping and securing apps using an SDK) uptake with MobileFirst Protect is low. It trails some other products in certain areas, particularly its lack of mobile app certificates (which are currently in development) and Security Assertion Markup Language (SAML) support, and it has limited app analytics capabilities.

Microsoft

Microsoft's EMM product is the Enterprise Mobility Suite. Microsoft Intune is a SaaS offering, which provides the core EMM capabilities.

- Intune's most compelling capability is its ability to manage mobile device access to Office 365. Intune has unique management functionality for the Office mobile apps, including the ability to restrict where users can save files (i.e., Save As) and its copy/paste policies. Intune also controls access to Office 365 without the need for a mobile access gateway.
- Microsoft enhanced Intune to manage the Outlook app for iOS and Android; however, this capability was not generally available during the review period for this report.
- The broader Enterprise Mobility Suite, which includes Azure Active Directory and Azure Rights Management, provides complementary functionality to Intune, such as Active Directory password reset on a mobile device, single sign-on (SSO), rights management and the management of SaaS applications; this complements Intune's ability to provision and manage mobile applications.

- Intune has two modes: stand-alone and Hybrid to Microsoft System Center Configuration Manager (ConfigMgr). The hybrid mode creates dependencies between Intune and ConfigMgr. Advanced administrative functionality requires Intune to be connected to ConfigMgr. However, new Intune functionality is not immediately available when it is connected to ConfigMgr, and changes to ConfigMgr can affect its ability to work with Intune. Microsoft plans to address this with the next major version of ConfigMgr.
- Intune supports most generic Android MDM APIs. It also has some Samsung Knox management capabilities. Intune does not support the Android for Work platform or other handset manufacturers (e.g., LG, HTC and MDM APIs).
- Intune's MAM module is new; it has limited capabilities and compatibility with third-party mobile application development tools.

MobileIron

MobileIron has one of the most complete EMM products. MobileIron's product strategy is to enable an "open" ecosystem of devices and mobile applications, and to protect access and information through server-side functions:

- MobileIron has strong policy management across iOS, Android and Windows Phone. It provides intuitive ways to set up complex policies.
- MobileIron's MCM product, Docs at Work, added data loss prevention (DLP) capabilities last year. Files that pass through Sentry cannot be read unless they are done so from an authorized device, user and app. It also provides file-auditing capabilities. Administrators can delete files from the console.
- MobileIron has put a heavy focus on integrating its MAM module, AppConnect, with third-party mobile application development platforms (MADPs), resulting in an ability to wrap applications from many MADPs, without the need to recompile. References also reported heavy use of AppConnect.
- MobileIron now has a secure PIM product for iOS and Android by licensing the iOS source code of Divide.
- MobileIron has two code bases: MobileIron Core and Cloud (SaaS-only); however, there is not feature parity between the two versions. Some features were added to the SaaS version first, and others are only available in Core. Organizations must ensure that they are evaluating the edition that meets their requirements.
- Monitoring the Core and Sentry server components is a challenge, and monitoring the MobileIron infrastructure is reactive. However, MobileIron has made monitoring enhancements, such as improved Simple Network Management Protocol (SNMP) monitors and Splunk integration.

SAP

SAP's EMM product is SAP Mobile Secure. This is a combination of Afaria (on-premises MDM), SAP MDM (SaaS-based MDM), SAP Mobile Place and SAP Mobile App Protection by Mocana (MAM), and SAP Mobile Documents (MCM/EFSS):

- Mocana is a well-known MAM vendor that works particularly well with an SAP mobile application strategy. Organizations can build and wrap applications quickly using SAP Fiori and Mocana.
- SAP is focused on supporting Android for Work, including the ability to wrap applications with AfW security capabilities to be deployed on pre-Android L devices.
- SAP Mobile Secure's reporting is strong. It provides visualizations and intuitive ways to create custom reports.
- SAP Mobile Secure consists of multiple consoles for MDM, MAM and MCM.
- Afaria customers reported difficulty limiting the number of devices a user can enroll. One organization created a custom-built work-around to address this issue.

Soti

Soti is an established vendor in the ruggedized device management space. Gartner typically finds Soti MobiControl among customers supporting Windows Mobile, WinCE and ruggedized Android devices:

- Soti's "Android+" approach enables customers to gain tight control and manageability of Android devices, without relying on handset-specific APIs.
- MobiControl provides advanced provisioning capabilities through bar code scanning for Windows Mobile, WinCE and Android.
- The Soti MAM SDK enables organizations to embed remote control functionality into mobile applications.
- Soti was one of the few vendors to have Samsung Knox references.
- SaaS platform is a dedicated instance model.
- MobiControl does not have a proprietary PIM offering; instead, it supports third-party offerings.
- Customers have reported instances of product instability, which has, at times, inhibited organizations from using MobiControl beyond ruggedized device scenarios.

Context

EMM suites help organizations integrate mobile devices into their security frameworks, systems and IT life cycles. Organizations use EMM tools to perform the following functions for their users:

- **Provisioning —** EMM suites configure devices and applications for enterprise use.

- **Auditing, tracking and reporting —** These products audit mobile devices and applications to track compliance with enterprise policies. They also maintain inventory for cost and asset management purposes and are capable of tracking the usage of services and apps.
- **Defense of enterprise data —** EMM suites enable administrators to apply technologies to encrypt data, control data flow and remotely revoke user access to mobile applications and information in the event the user or device becomes untrusted (e.g., through device loss, unauthorized reconfiguration or employee termination).
- **Support —** EMM suites help IT troubleshoot mobile device problems through inventory and analytics, as well as by invoking remote actions.

Product/Service Class Definition

Four core EMM technical categories help IT organizations perform the relevant services (there are some overlapping capabilities among these categories):

1. **MDM —** This platform life cycle management technology provides inventory, OS configuration management, mobile app provisioning and deprovisioning, as well as remote wipe and viewing/control for troubleshooting. MDM profiles installed on the device facilitate these functions.
2. **MAM —** This technology applies management and policy control functionality to individual applications, which are then delivered via enterprise app stores and managed locally on devices via the EMM console. This capability is necessary when the OS does not provide adequate management or security capability or when organizations elect not to install an MDM agent on the device. MAM can also provide analytics capabilities to help administrators and application owners understand usage patterns. MAM and MDM functions may be also used complementarily. There are two basic forms of MAM:
    - **Preconfigured applications —** EMM vendors provide proprietary mobile apps or integrate with particular third-party apps to provide enhanced levels of manageability. These most commonly include productivity and collaboration applications, such as secure PIM for email, calendaring and contact management, as well as a secure browsers provided by the EMM provider or a third party.
    - **Application extensions —** These apply policies to applications through the use of an SDK or by wrapping.
3. **Mobile identity —** EMM tools help ensure that only trusted devices and users access enterprise applications. Mobile identity capabilities may use one or more of the following technologies:
    - User and device certificates
    - App code signing
    - Authentication
    - SSO

EMM tools are increasingly using contextual information (e.g., location and time) to help inform access decisions.

4. **MCM —** This enables users to access content from their mobile devices. The MCM function in EMM suites has four fundamental roles:

   - **Content security —** A client-side app enables users to store content securely on mobile devices. The EMM can enforce policies such as authentication, file sharing and copy/paste restrictions. Content comes from sources such as email (i.e., attachments), files accessed from a back-end repository or files accessed from a cloud repository.
   - **Content access —** This is a connection to a back-end repository, where users can pull content to their devices.
   - **Content push —** These capabilities involve push-based file distribution, replacement and deletion.
   - **File-level protection —** EMM tools are not full-blown DLP or information rights management (IRM) products; however, they may apply file-level protections in certain mobile contexts, and they may integrate into larger frameworks.

Critical Capabilities Definition

EMM vendors have different strategies for addressing the need to secure and enable enterprise mobility. EMM suites continue to broaden and must be updated regularly. Consequently, EMM suites cannot excel at all functions.

Secure PIM

This client-side app provides email, calendaring and contact management. This is important because built-in email clients on mobile devices may have insufficient security, may require users to be managed via a MDM tool or the organization may want to support PIM consistently across platforms.

In this category, we look at depth of policy support, breadth of platform support and email functionality. Many organizations struggle with secure PIM products, mostly due to usability challenges. The EMM vendors have demonstrated that it's hard to build a secure PIM product. Usability issues, rather than lack of policy control, are the biggest inhibitors to adopting a secure PIM product.

Secure Content Access/Distribution

Mobile users have a variety of content needs. EMM suites provide a baseline of MCM functionality, although some vendors also provide full file share and sync products. In EMM toolsets, we look at products' ability to enable secure access to enterprise content, document push/pull and DLP functions.

Client Management

Windows PCs and Macs have added MDM APIs, which support lightweight forms of management. The following are some of the functions MDM tools can provide for Windows 8.1 and Mac OSX clients: inventory, remote wipe, Wi-Fi and email configuration, OS version control and app delivery.

Today's PCs support a mix of MDM and legacy management for Win32 applications and subsystems. Although less common, some vendors in this space also provide legacy client management capabilities as well, including patch management, software distribution, software usage monitoring, and security configuration assessment.

Administration and Usability

Accessibility for IT administrators is important to the successful use of EMM products. This capability considers the ease of using the product, language support, integration of various EMM modules and product reputation during situations such as implementations and upgrades.

Mobile App Management

This involves applying policies directly to mobile applications, rather than applying them through OS management controls. This is required when the OS lacks particular security or management capabilities, or when organizations want to limit the presence of a management agent on a user's device.

Here, we evaluate the depth of policies, breadth across platforms and the list of public app store apps that the MAM product can support.

Mobile User Support

Mobile operations is becoming more important, as mobile devices are used increasingly for mission-critical purposes. These capabilities look at remote screen capture, remote control and mobile analytics to help administrators support end users and assess the quality of mobile services.

Mobile Identity and Access

Mobile identity and access capabilities evaluate certificate management, authentication, SSO, VPN, integration with NAC products, integration with IAM tools, and other capabilities that enable contextual authentication.

Device Security and Compliance

EMM suites enforce policies that protect enterprise data and the network. Smartphones and tablets come with many features that EMM suites can exploit to help organizations secure mobile devices. Here, we look at the breadth and depth of policy support at the device and OS level.

Device Configuration Management

In addition to device security and compliance, organizations also manage device configurations to automate tasks for end-user convenience and IT operational efficiency. This capability evaluates the EMM vendor's ability to provision and manage device configurations across a wide range of platforms.

Architecture and Scalability

This evaluates the products' ability to support a large number of mobile devices, centrally, with relatively few servers. It is affected by the number of devices, the breadth of functionality used and the geographic dispersion. Scale has been unproved in this market.

We looked at the architecture of the products, their support for high availability in critical parts of the infrastructure and the tools' ability to be monitored by standard enterprise communications application (ECA) tools (e.g., Microsoft System Center Operations Manager).

Cloud Offering

SaaS has been widely adopted by EMM customers. Because most products originated as on-premises offerings, their SaaS products may be identical to the on-premises versions. True multitenancy is the most important factor to consider.

In this model, the EMM platform runs all tenant instances in a shared space, and one database management system (DBMS) instance is used to hold the data of all tenants. The EMM platform multitenancy features control all resources (e.g., DBMS) offering maximum potential elasticity. The benefits to customers include rapid product releases, no need to maintain your EMM instance and analytics derived from the other customer tenants in the vendor's SaaS environment. There are other SaaS variations, such as shared-database, shared-processing, shared-hardware and shared-nothing multitenancy. Other important factors in the cloud offering include the number of data centers the vendor uses to operate the SaaS offering, certifications and SLAs.

Use Cases

This year, Gartner identified six use cases for EMM suites, each with its own requirements. Use cases are not mutually exclusive, so several of them may apply to a particular organization.

Global Enterprise Deployment

As EMM becomes a more established IT operations technology, global organizations will manage their environments centrally.

Global organizations support a broad range of devices and applications, and have a broad range of requirements. This requires scalability and a complete set of capabilities.

Regulated Industries

Organizations that are subject to stringent data security regulations require EMM capabilities that have a strong focus on data protection.

The following capabilities are heavily weighted in this use case:

- Secure PIM
- MAM
- Device security and compliance
- Certifications obtained for secure use of data in the EMM vendor's product or architecture

Unified Endpoint Management

Organizations are looking to EMM tools for lightweight support for PCs. Windows 8 and Mac OSX have added increased MDM policy support, and the trend continues with Windows 10.

This use case looks at the vendor support for MDM functions, as well as traditional client management functionality, to do security configuration assessment, patching, software distribution and remote control. This use case weighs client management most heavily.

Special-Purpose Device Support

In this situation, organizations have a specific use case for a mobile device. The organization chooses a device that is best-suited to that purpose.

The device used is often Android and, increasingly Windows, tablets, because of their ability to be configured for a particular purpose. Here, the following capabilities are weighted most highly:

- **Device configuration management —** specifically the EMM vendor's ability to support Android hardware models.
- **Mobile user support —** vertical use cases often involve the need for troubleshooting or more-complex configurations.
- **Document distribution —** this is often an important capability.

SaaS Deployments

SaaS has been widely embraced by EMM buyers. This use case weighs the cloud offering capabilities most heavily.

Line-of-Business App Support

Mobile applications are becoming more critical. This use case emphasizes MAM and mobile user support capabilities.

Vendors Added and Dropped

Added

- BlackBerry
- Microsoft

Dropped

No vendors were dropped this year.

Inclusion Criteria

The inclusion criteria are more rigorous than those used in the "Magic Quadrant for Enterprise Mobility Management Suites":

- EMM revenue of $35 million in 2014
- EMM support for iOS, Android and Windows Phone
- The EMM vendor must provide MDM, MAM through an app wrapping or SDK, and MCM

Table 1. Weighting for Critical Capabilities in Use Cases

Critical Capabilities	Global Enterprise Deployment	Regulated Industries	Unified Endpoint Management	Special-Purpose Device Support	SaaS Deployments	Line-of-Business App Support
Secure PIM	8%	17%	3%	2%	8%	8%
Secure Content Access/ Distribution	8%	5%	3%	10%	3%	10%
Client Management	5%	0%	40%	0%	5%	0%
Administration and Usability	10%	5%	10%	5%	8%	10%
Mobile App Management	10%	18%	3%	3%	8%	22%
Mobile User Support	8%	8%	8%	13%	5%	16%
Mobile Identity and Access	10%	10%	8%	5%	10%	8%
Device Security and Compliance	10%	20%	8%	20%	10%	8%
Device Configuration Management	10%	5%	9%	24%	8%	8%
Architecture and Scalability	16%	10%	3%	8%	5%	5%
Cloud Offering	5%	2%	5%	10%	30%	5%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**
As of May 2015						

Source: Gartner (June 2015)

This methodology requires analysts to identify the critical capabilities for a class of products/ services. Each capability is then weighed in terms of its relative importance for specific product/ service use cases.

Critical Capabilities Rating

Each of the products/services has been evaluated on the critical capabilities on a scale of 1 to 5; a score of 1 = Poor (most or all defined requirements are not achieved), while 5 = Outstanding (significantly exceeds requirements).

To determine an overall score for each product in the use cases, the ratings in Table 2 are multiplied by the weightings shown in Table 1. These scores are shown in Table 3.

Table 2. Product/Service Rating on Critical Capabilities

Product or Service Ratings	AirWatch by VMware	BlackBerry	Citrix	Good Technology	IBM	Microsoft	MobileIron	SAP	Soti
Secure PIM	3.2	2.8	4.1	4.5	3.2	1.0	3.2	2.0	2.0
Secure Content Access/ Distribution	3.9	3.2	4.5	3.8	3.6	3.5	4.2	3.0	3.0
Client Management	3.6	1.0	2.5	2.0	4.4	4.9	2.8	2.5	3.2
Administration and Usability	4.2	4.0	3.5	2.8	3.7	2.8	3.8	2.5	3.0
Mobile App Management	3.8	2.9	4.1	4.8	3.0	2.5	4.0	3.7	3.5
Mobile User Support	3.0	2.5	3.5	4.3	3.0	2.0	3.3	2.0	4.7
Mobile Identity and Access	3.5	3.5	3.8	3.8	4.0	4.2	4.2	3.0	3.5
Device Security and Compliance	4.0	4.9	3.8	3.0	3.7	3.2	4.0	3.6	3.7
Device Configuration Management	4.2	4.0	3.3	2.0	4.0	4.0	3.8	3.1	4.8
Architecture and Scalability	4.4	4.5	3.0	4.0	3.7	3.0	3.8	4.0	3.8
Cloud Offering	4.2	3.0	3.0	2.5	4.8	4.8	4.0	3.5	3.5
As of May 2015									

Source: Gartner (June 2015)

Table 3 shows the product/service scores for each use case. The scores, which are generated by multiplying the use case weightings by the product/service ratings, summarize how well the critical capabilities are met for each use case.

Table 3. Product Score in Use Cases

Use Cases	AirWatch by VMware	BlackBerry	Citrix	Good Technology	IBM	Microsoft	MobileIron	SAP	Soti
Global Enterprise Deployment	3.87	3.53	3.57	3.51	3.68	3.16	3.78	3.09	3.57
Regulated Industries	3.76	3.60	3.78	3.83	3.50	2.75	3.80	3.09	3.43
Unified Endpoint Management	3.75	2.58	3.16	2.79	3.99	3.89	3.42	2.77	3.51
Special-Purpose Device Support	3.92	3.76	3.57	3.15	3.77	3.38	3.85	3.12	3.93
SaaS Deployments	3.91	3.33	3.45	3.19	3.99	3.60	3.83	3.13	3.51
Line-of-Business App Support	3.75	3.35	3.76	3.79	3.49	2.88	3.81	3.00	3.61
As of May 2015									

Source: Gartner (June 2015)

To determine an overall score for each product/service in the use cases, multiply the ratings in Table 2 by the weightings shown in Table 1.

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Magic Quadrant for Enterprise Mobility Management Suites"

"How Products and Services Are Evaluated in Gartner Critical Capabilities"

"Toolkit: Enterprise Mobility Management RFI and RFP Template"

Critical Capabilities Methodology

This methodology requires analysts to identify the critical capabilities for a class of products or services. Each capability is then weighted in terms of its relative importance for specific product or service use cases. Next, products/services are rated in terms of how well they achieve each of the critical capabilities. A score that summarizes how well they meet the critical capabilities for each use case is then calculated for each product/service.

"Critical capabilities" are attributes that differentiate products/services in a class in terms of their quality and performance. Gartner recommends that users consider the set of critical capabilities as some of the most important criteria for acquisition decisions.

In defining the product/service category for evaluation, the analyst first identifies the leading uses for the products/services in this market. What needs are end-users looking to fulfill, when considering products/services in this market? Use cases should match common client deployment scenarios. These distinct client scenarios define the Use Cases.

The analyst then identifies the critical capabilities. These capabilities are generalized groups of features commonly required by this class of products/services. Each capability is assigned a level of importance in fulfilling that particular need; some sets of features are more important than others, depending on the use case being evaluated.

Each vendor’s product or service is evaluated in terms of how well it delivers each capability, on a five-point scale. These ratings are displayed side-by-side for all vendors, allowing easy comparisons between the different sets of features.

Ratings and summary scores range from 1.0 to 5.0:

1 = Poor: most or all defined requirements not achieved

2 = Fair: some requirements not achieved

3 = Good: meets requirements

4 = Excellent: meets or exceeds some requirements

5 = Outstanding: significantly exceeds requirements

To determine an overall score for each product in the use cases, the product ratings are multiplied by the weightings to come up with the product score in use cases.

The critical capabilities Gartner has selected do not represent all capabilities for any product; therefore, may not represent those most important for a specific use situation or business objective. Clients should use a critical capabilities analysis as one of several sources of input about a product before making a product/service decision.

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp