Description of document:	US Census Bureau internal agency records which discuss the merits of iPads and/or similar pad/tablet computer devices for agency employee use, 2011
Requested date:	25-August-2011
Released date:	08-November-2011
Posted date:	28-November-2011
Date/date range of document:	13-April – 28-September-2011
Source of document:	FOIA Office U.S. Census Bureau, Room 8H027 4600 Silver Hill Road Washington, DC 20233-3700 Fax: 301-763-6239 (ATTN: FOIA Office)

UNITED STATES DEPARTMENT OF COMMERCE
Economics and Statistics Administration
U.S. Census Bureau
Washington, DC 20233-0001
OFFICE OF THE DIRECTOR

NOV 0 8 2011

This is in further response to your request to the Department of Commerce, U.S. Census Bureau. Our office received your initial request on August 25, 2011 for "a copy of internal agency (Census Bureau) memos or other correspondence or documents that review or discuss the merits and/or disadvantages of iPads and similar pad/tablet computer devices for employee use." On September 22, 2011, our office sent you a fee estimate of $3875.88 for processing your request.

On September 26th, our office received a revised request from you indicating that you would accept whatever records were available as a result of checking with Scott D. Williams and Gary K. Sweely and retrieving those records that were readily accessible to them and retrievable with one hour or less of search time each. You also narrowed the scope of your request to the Ipad evaluation test conducted by Census including participation by Mr. Williams and Mr. Sweely. We assigned tracking number 11-364 to this request. We are responding under the Freedom of Information Act (FOIA).

According to Mr. Sweely, he does not have any materials, and was not involved in any work regarding the Ipad evaluation testing. This has been confirmed by Scott Williams. Therefore, the two hours of searching was limited to Mr. Williams.

Mr. Williams specifically identified the documents that were in his possession and responsive to your request to be:

1. Meeting minutes, Mobile Device Management Team;
2. Draft policy for Mobile Device Management;
3. His notes for Census Mobile Conference Discussion; and
4. Mobile Device Management production criteria.

He also stated that his office has no specific documentation of Tablet/Ipad evaluation.

Enclosed are the documents responsive to your request. There is no charge for this information.

Sincerely,

Dana Cope
Chief, Freedom of Information Act and Information Branch

Enclosures

Direction/Roadmap of Enterprise Mobile Management
Notes for Census Mobile Summit September 28, 2011
Scott Williams

1. Government Furnished Smartphones/Pads:

BlackBerry's: We will continue to furnish Verizon BlackBerry Products for the coming year. Bold Touch available next quarter.

NEW Playbooks and iPad's: Loaner Program for those needing BlackBerry Playbook and Apple iPad (currently piloting limited number), limited number of production loaners avail by Thanksgiving.

We will be adding a Loaner Pad Request to the Remedy application, similar to the Loaner Laptop Request program.

All government furnished devices will have security baselines installed and managed by the enterprise MDM's and are subject to being wiped if needed.

Mobile Devices for Research and Test (R+T): These requests will be Proposed to the CTO's office and managed within the Center for Applied Technology (CAT). Most mobile devices on the market (Android and Windows OS' etc) are likely to be favorably considered for CAT R+T purposes.

2. Verizon 3G in-Building Enhancements and WiFi Coverage:

NEW Verizon 3G coverage is available throughout the Census HQ Building.

You will get the best service for your cell phone in HQ if your carrier is Verizon.

WiFi Coverage is available through HQ and we are currently outfitting NPC with full WiFi coverage, with goal of activating wifi throughout Census locations.

3. NEW Employee WiFi Availability:

IT has established a new WiFi capability for employee access called Employee WiFi to the Internet from their Loaner GFE devices and Personal devices.

Provide Username (James Bond Id) and Network Password from your government furnished mobile device and you're on. It's System-11 for those that haven't used it yet.

We are assessing the use of Employee WiFi for personal devices.

4. Mobile Device Management:

BES MDM: We will continue using BlackBerry Enterprise Server (BES) to manage BB's and Playbook's.

NEW AFARIA MDM: We have just operationalized the Sybase AFARIA product in production to manage the iPads and in the CAT to manage R+T of devices.

We will monitor the MDM market as it matures with goal of one MDM for ALL devices.

5. Available Now Internet Access and iNotes Email, Coming Soon Virtual Desktop Infrastructure (VDI) Access from your Mobile Device:

Government Furnished and Personal Mobile Devices can be used to access the Internet from WiFi, or 3G, and the iNotes email Application remotely.

We are currently developing VDI technology that provides remote access to your desktop. This will initially be available for Government Furnished Mobile Devices.

There will not be direct access to the Census secure network from mobile devices.

6. Market Place for Applications:

Production BB's will receive managed Apps only from the BES.

Loaner iPad Apps can be downloaded from the Apple Store with iTune cards for the immediate future.

The MDM in the CAT can be used to simulate a "Private App Market" to develop and push Apps to the CAT R+T devices.

INFORMATION TECHNOLOGY DIRECTORATE

Interim Mobile Device Management and Acquisition Policy

PURPOSE

The purpose of this policy is to provide interim guidance regarding acquisition, management, control and use of mobile devices at the U.S. Census Bureau.

BACKGROUND

Use of mobile devices has grown rapidly over the past few years and the Census Bureau recognizes the value of exploiting this emerging technology for our own business use as well as a vehicle to communicate more effectively with our customers. The speed at which this technology has grown necessitates that we quickly establish an interim methodology for effectively managing how it will be used at Census and for protecting our network infrastructure from compromise and preventing loss or corruption of data.

Our current mobile device environment consists mainly of BlackBerry smartphones, cellular phones, and cellular broadband aircards. We have begun to expand this capability to include various tablet PCs and other non-BlackBerry devices such as Apple iPads, Playbooks, and Xooms.

The principal business needs with regard to use of mobile devices at Census include:

- For testing Census-developed mobile applications to be run on the various device-specific mobile operating systems (e.g., Android, iOS, webOS, Symbian, and others) used by the general public,
- To enhance Census Field Representative data collection by enabling use of contemporary mobile communications/computing device technology, and
- To satisfy routine business and mobile communications requirements (as is the current case with BlackBerry smartphones)

SCOPE

This policy applies to all Census Bureau purchased or furnished mobile devices.

For the purpose of this interim policy, mobile devices are defined as tablet PCs (such as Apple iPads, Motorola Xooms, BlackBerry Playbooks), BlackBerry and other similar smartphones.

This policy is aimed particularly at facilitating the use of tablet PCs and similar mobile technology devices, but will be extended to all such devices that are capable of connecting to the Census IT network and/or that employ cellular broadband communications.

With the exception of any on-board or add-on cellular broadband capabilities, this policy does *not* apply to laptop computers provided by the IT Directorate under the LTSO-managed long- and short-term loaner program which is controlled and managed separately.

EFFECTIVE DATE

This policy is effective upon signature.

POLICY

Acquisition and Issue of Devices

Acquisition of all mobile device hardware and mobile software (i.e., mobile applications) to be used at the Census Bureau Headquarters and Regional Offices as Government-owned property, shall be centrally approved by the IT Directorate and acquired by the Telecommunications Office (TCO) on behalf of all Census Program Areas.

Current Constraints

No mobile device will be made available to individual users for routine business use until a Mobile Device Management (MDM) tool is in place.

No mobile devices will be granted access to the Census Bureau production network until it is has been certified and accredited in a Security Plan.

Authority

The IT Directorate (ITD) will work with all Census Directorates to determine which new devices and mobile operating systems (OS) to deploy and support at the Census Bureau.

The ITD shall maintain a list of approved:

- Mobile devices
- Mobile OS's
- Security standards
- Development standards for mobile applications
- Evaluation criteria for acquiring commercially available mobile applications
- Mobile applications and usage guidance

Rules of Behavior and Acceptable Use of Mobile Devices

Until an updated, more mobile device-specific policy is developed and approved, Census Bureau employees and contractors who are issued a government-owned mobile device must adhere to existing policies established for acceptable use of Census Bureau IT systems as well as BlackBerry Policies and User Guidelines.

Once published, users will be required to sign an acknowledgement of receipt and acceptance of the Census Bureau mobile device policies and user guidelines. The mobile device policies and user guidelines document will provides details regarding the proper use and security of the device, and will be maintained by TCO.

Security Requirements

The IT Directorate will own and maintain all security related documentation required by applicable laws and regulations, for mobile devices and the device operating system only. Software developed by Census Bureau Program Areas for mobile device platforms will require security certification and accreditation in accordance with Census Bureau IT Security Program Policy (ITSPP).

IMPLEMENTATION

Mobile Devices Available for Testing Public-Use Mobile Apps

The IT Directorate will be responsible for maintaining a current inventory of mobile devices in the Center for Applied Technology (CAT). These devices will be kept in the CAT and will only be allowed to connect to the Internet through the Census Bureau's Non-Production Employee Wireless network and the Guest Wireless network.

The CAT will secure and maintain an inventory of mobile devices on the leading commercially available operating systems, for use within the CAT. A current inventory list will made available to Census users.

All Census Bureau staff that needs to perform testing on a mobile device can do so by entering a Remedy ticket reserving the requested devices for application testing.

Mobile Devices and Applications for Customer Use Within the Census Bureau

Initially, non-Blackberry mobile devices and mobile applications will not be supported by the IT Directorate outside of the CAT. Only when a centralized Mobile Device Management infrastructure has been implemented, and the required security controls have been put in place and documented in an approved System Security Plan will devices with a business objective be supported outside of the CAT. Until such time, test and evaluation shall be conducted exclusively in the CAT.

RELATED DOCUMENTS

- Software Acquisition Policy for Census Bureau Employees and Contractors, April 16, 2008

- Acceptable Use Policy for U.S. Census Bureau Information Technology Systems, February 17, 2009
- Data Stewardship Policy DS-007 "Information Security Management Program," May 27, 2009
- Department of Commerce Policy on Electronic Transmission of Personally Identifiable Information, July 30, 2009
- Census Information Technology Hardware Acquisition Policy, February 1, 2010
- Executive Order 13513, "Federal Leadership on Reducing Text Messaging While Driving," October 1, 2009
- BlackBerry Policies and User Guidelines, September 30, 2010.

POLICY OWNER

The Chief of TCO is responsible for maintaining implementing, and disseminating this policy.

This interim policy will undergo further review and revision in the near future as the Census Bureau takes a more comprehensive view of mobile communication/computing devices and more definitive policy is developed regarding acceptable use of this technology.

SIGNATURE

BRIAN E. MCGRATH
Associate Director for Information Technology /
Chief Information Officer

Summary Information	
Policy Title:	Interim Mobile Device Management and Acquisition Policy (DRAFT)
Date Signed:	
Policy Owner:	Chief of the Telecommunications Office (TCO)
Office Responsible for Implementation:	Center for Applied Technology (CAT)
Office Responsible for Dissemination:	Center for Applied Technology (CAT)
Stakeholder Vetting:	CAT, ITSO, TCO, LTSO, ISSRO, Field TMO, OAES

Attachment 1

Mobile Device Management Meeting Notes

Wednesday, May 25, 2011, 9:00 – 10:00 AM
Room: 4K042

Invitees (*Denotes in attendance)

TCO	Other:	Guests:
Roger Rhoads	Barry Sessamen/DIR *	
Kenneth Harrison	Adeeb Parkar/ITSO *	
Ross George *		
Ken McCathran *		
Hadi Tambal		
Kimberly Vines-Weathers *		

Agenda

1. Introduction
    a. Identify team members and roles

2. Project Scope
    a. Requirements/Business Need
    b. Tablets/Platforms to be included (iPad, PlayBook, Xoom, etc)
    c. Secure configuration/Centralized management of devices
    d. RFI out to vendors

3. Future Meeting Topics

Meeting Notes:

The group agreed a policy is needed as a first item. Barry has been working on a policy document and will send the draft out for review/comment.

Adeeb will check with Commerce to see what they have in terms of an existing policy for mobile devices.

The group discussed three main user groups:

1. General Census users accessing Census apps and data
2. Census employees using devices for data collection
3. External users accessing Census provided applications

In addition, the group discussed two main application types:

1. Generally available off-the-shelf applications
2. Custom Census applications developed internally

Barry noted he has received requests from Lisa Wolfisch and Jeremy Wu regarding mobile apps/services. The group talked about establishing a Mobile Working Group, which could include members outside of IT. The working group would review requests for testing devices in the Center for Applied Technology (CAT) and make recommendations based on the test results.

There will be a number of challenges with managing the devices. The iPads/iPhones, for example, are managed via iTunes, which requires a credit card on file. The group will need to determine how multiple devices can be setup and maintained in such a scenario. There are also questions regarding which group will be responsible for publishing applications to the iTunes, and potentially other online stores.

Mobile Device Management Meeting Notes

Wednesday, June 1, 2011, 9:00 – 10:00 AM
Room: 4K042

Invitees (*Denotes in attendance)

TCO	Other:	Guests:
Roger Rhoads	Barry Sessamen/DIR *	
Kenneth Harrison	Adeeb Parkar/ITSO *	
Ross George		
Ken McCathran *		
Hadi Tambal *		
Kimberly Vines-Weathers *		

Meeting Notes:

Barry provided a draft policy document, and we have received comments which will be incorporated into the next draft. The document will be more of guidelines instead of a formalized policy.

Adeeb presented a draft chart showing the CIO's Mobile Device Policy. It was divided into three groups: BlackBerry, IOS, and Android devices. The current DOC policy on devices covers only BlackBerry devices while on foreign travel.

There are number of challenges with managing the devices, particularly with setting up an iPad or iPhone, as it requires going through iTunes.

Adeeb has a prototype secure configuration for the iPad, and demonstrated how it works at his desk after the meeting.

The group discussed amending the current IT hardware purchase process to include configuration of the device(s) by IT prior to being delivered to the customer. The device would potentially be added to a user's accountable property and be tracked in Remedy.

Wireless access inside Census was also discussed. The group felt access to the Guest Wireless network would be more secure than allowing access to the Production Wireless network. A separate policy for granting Census employees, with Census-provided devices, access to the Guest Wireless network would be needed.

With the coming of VDI and internally developed applications, the group felt we need to establish firm guidelines up front before devices are procured for and delivered to customers.

Meeting Minutes

Subject	Mobile Device Management (MDM) Weekly Status Meeting	Date	Wednesday, June 8, 2011
Facilitator	Ken McCathran	Time	9:00 AM
Location	4K045	Scrivener	Ben Llewellyn
Attendees	Ken McCathran, Hadi Tambal, Kenny Harrison, Barry Sessamen, Adeeb Parkar,		
	Ben Llewellyn		

- Acronyms are listed at the end of these minutes.

1. CAT Device Management

- CAT devices will be owned, managed and maintained by TCO.
- The CAT will use the model of a laboratory, not a lending library.
  - The room will be locked and require an appointment for entry.
  - No one will be allowed to check a device out of the CAT; all work must be done in the room.
  - The CAT is currently locked via card reader, and only those engaged in CAT projects will have direct badge access.
  - Visitors who wish to use the CAT for testing mobile apps may need to make an appointment.

- The proposed starting inventory will be the following:

Phones (2 each) 3G or 4G technology	Tablets (3 each) Wi-Fi only
iPhone 4	iPad 2
Droid X	Motorola Xoom
HTC Thunderbolt	Samsung Galaxy
Android (most basic model)	BlackBerry PlayBook

2. Requests

- Yesterday, a related group called Mobile Devices/Apps met with representatives of LED (part of LEHD, which in turn is part of CES).
  - LED made a formal request for two iPads.
  - These would be used in continued development of LED's *OnTheMap* app.
  - This request is Category 1a (see Security).

3. Security

- There are three general reasons why a developer would need access to the CAT:
  - The need to simulate user experiences for a system that is in place for data dissemination
  - The need to simulate user experiences for an app being created for data dissemination
  - The need to access internal production resources.

- The three types of access requests are:
  - 1A – CAT only – Wi-Fi Guest (System 10)
  - 1B – CAT only – Access to resources such as databases (System 19)
  - 2 – Access to the Production Network (System 1)

- The CAT will not touch Census production data.

- Kenny noted that we will need to change the policy to allow certificates on iPads, etc. with limited circumstances. We will need a ruling on this from ITSO.
  - Kenny will update the Guest Wireless Security Policy to accommodate the CAT.
  - Adeeb asked him to give the updated policy to Ellen Soper of ITSO for comments.

4. One IT

- We need to propose initiation of an MDM team to the CIPR Board:
  - TCO would serve as technical lead.
  - TMO would serve as business lead.
  - Other groups would be added as needed.

- Adeeb will create a purchasing grid for the proposed starting inventory:
  - All hardware requests must go through ISSRO.
  - CTO would be the requester.

5. Risks and Issues

- Kenny noted the eventual risk of CAT customers hacking into Census data.
  - At the moment, this risk is negligible, because there will only be access to the Guest network.
  - The risk will eventually grow as public needs expand.

6. Action Items

- Kenny will update the Guest Wireless Security Policy to accommodate the CAT (6/22).
- Barry and Adeeb will formally brief the Division Chiefs on the existence of the CAT and its policies (6/15).
- Adeeb will create a purchasing grid for the proposed starting inventory (prior to 6/15).
- Barry and Adeeb will conduct procurement (6/15).

ACRONYMS:

CAT = Center for Applied Technology
CES = Center for Economic Studies
CIPR = Census IT Project Review
CTO = Chief Technology Officer
ISSRO = Information System Support and Review Office
ITSO = Information Technology Security Office
LED = Local Employment Dynamics
LEHD = Longitudinal Employer-Household Dynamics Program
MDM = Mobile Device Management
TCO = Telecommunications Office
TMO = Technologies Management Office

Meeting Minutes

Subject	Mobile Device Management (MDM) Weekly Status Meeting	Date	Wednesday, June 15, 2011
Facilitator	Ken McCathran	Time	9:00 AM
Location	4K045	Scrivener	Ben Llewellyn
Attendees	Ken McCathran, Hadi Tambal, Kimberly Vines-Weathers, Adeeb Parkar, Udaya Chundury,		
	Ben Padilla, Ben Llewellyn		

- Acronyms are listed at the end of these minutes.

1. Draft Policy Documents

- Ken noted that Barry Sessamen has updated the draft policy related to MDM.
  - Devices would be kept in either the CAT or the usability lab for security reasons.
  - Udaya noted that some customers may have legitimate business need for a long-term loaner program, similar to the one for laptops. This service may eventually be in place, but it is not the first goal.

- He also noted that Kenny Harrison is preparing a new restricted network dedicated to CAT-related equipment
  - This is separate from the existing Guest Wireless Network.

- There was some discussion as to whether we will need a policy or guidelines.
  - It was agreed that we must prepare guidelines ASAP to fill the immediate need.
  - Ross George is presently working on an actual policy.

- The SAP and the SLIC must be followed/used when procuring apps.
  - There was some question as to whether or not ISSRO has a policy for letting customers buy apps with a purchase card, or if ISSRO will do something along the lines of providing the customers with iTunes cards. No answer was forthcoming.
  - Concern was expressed that we not create policies that contradict one another or make the purchase process convoluted due to multiple policies.

- Udaya said that CTO is creating a Standards Working Group, which may eventually determine which apps are acceptable.
  - That group will include participants from every Census Directorate, also including TMO.
  - Their first priority is Oracle.

- Ben P. expressed concern that multiple groups are duplicating each other's work, but Adeeb noted that the Standards group only looks at existing technology, while the MDM group looks at creating new technology.

- Hadi noted that we must find ways of distinguishing Government vs. personal data for mobile devices.

2. MDM Vendors/Testing in CAT

- Ken noted that ACQ requires studies—which can take six months or longer—before full-scale purchasing can begin, but our customers are clamoring for these devices now.

- We are looking at five potential vendors for an MDM System:
  - Sybase
  - AirWatch
  - Good Mobile Control
  - MobileIron
  - Ubitexx (recently purchased by RIM)

- Representatives from Ubitexx will present their system at next week's meeting.
  - Ken will contact AirWatch and Good for future presentations.
  - Adeeb will contact MobileIron for a future presentation.
  - No one has committed to contacting Sybase; Udaya noted that it is already in use for Field Operations.

- It was noted that many of the vendors allow organizations to use a limited number of devices as a pilot.
  - Unsure if Sybase does this, but the others do.
  - TCO generally gets evaluation licenses for 10-20 users, for 30 days.

- Udaya will set up a meeting between Ken and TMO, to see about combining forces on this effort.

- It was agreed that we should be sure to list limitations of each device to customers requesting them (e.g., iPads do not use Flash or Java).

- It was also noted that Apple charges a fee to app developers.

- A summary of Government-created apps that are available via the App Store can be found at http://www.data.gov/.
  - It was agreed that it would be a good idea to contact app developers at other agencies to see what information we could leverage.
  - Udaya noted that the Census did this when evaluating Sharepoint.
  - Ken will elevate this subject to Brian McGrath.

3. Future Meeting Topics

- Next week's meeting will be devoted to the RIM presentation.

5. Risks and Issues

- No new risks or issues identified.

6. Action Items

- Udaya will arrange a meeting between TMO and Ken McCathran to discuss vendors and licensing (6/22).
- Ken will elevate to Brian McGrath the possibility of contacting app developers at other Government organizations (6/22).
- Ken will arrange a demo from AirWatch and Good Mobile Control (6/29).
- Adeeb will arrange a demo from MobileIron (6/29).

ACRONYMS:

ACQ = Office of Acquisitions
ASAP = As Soon as Possible
CAT = Center for Applied Technology
CTO = Office of the Chief Technology Officer
ISSRO = Information System Support and Review Office
MDM = Mobile Device Management
RIM = Research in Motion
SAP = Software Acquisition Policy
SLIC = Software License Information Center
TCO = Telecommunications Office
TMO = Technologies Management Office

Meeting Minutes

Subject	Mobile Device Management (MDM) Weekly Status Meeting	Date	Wednesday, June 22, 2011
Facilitator	Ken McCathran, Soo Lee (RIM)	Time	9:00 AM
Location	4K045	Scrivener	Ben Llewellyn
Attendees	Ed Antonio (TMO), Daren Gutschow (TCO), Ken McCathran (TCO), Jae Pak (TCO),		
	Adeeb Parker (ITSO), Geof Pejsa (TMO), Roger Rhoads (TCO), Thad Schmidt (TMO),		
	Barry Sessamen (IT/CIO), Derek Spurlock (TMO), Hadi Tambal (TCO),		
	Kimberly Vines-Weathers (TCO), Ben Llewellyn (TCO)		

- Acronyms are listed at the end of these minutes.

1. Guest Speaker

- Ms. Soo Lee from RIM was the guest speaker. She had been invited to discuss MDMs offered by her company.
  - Fuse will be available in August or September (more likely September).
  - Until Fuse is ready for launch, Ubitexx is the free "product preview" version.

- She also noted other upcoming products from RIM:
  - New Playbook with Wi-Fi will be available in August.
  - Winmaxx for Sprint will include Wi-Fi and 4G.
  - LTE for Verizon will likely be available at the end of CY2011.
  - BlackBerry 7 will be the last BlackBerry OS. After that will be full cutover to QNX, which she said would not be backward compatible.
  - BlackBerry Balance will allow customers to have both personal and professional information on separate, firewalled sides of the device, to keep each from compromising the other.

2. Q&A

During the week after, Ms. Lee provided Mr. McCathran with written responses to questions asked during the meeting.

- Can you get more than 10 licenses on the Ubitexx preview?
  - We would be able to get you additional licenses, but know that there is no migration path from the Ubitexx preview to our production solution that will be released this fall. **Please let me know if you would like to proceed with additional licenses.**

- Geo-Fencing and Cookie-Crumb tracking on PlayBook?
  - This is a 3rd party solution such as ActSoft (www.actsoft.com) that can do geo-fencing and trails. **I'd be happy to ask them to come in and present their solution to you.** I have many clients that have already bought into their solution.

- Can Ubitexx track Android 3.0 and iOS 5?
  - Yes.

- Can Ubitexx manage Wi-Fi only devices?
  - Yes.

- Can Ubitexx tell if the iOS/Android has been jail-broken?
  - This is under product review. We would need an agent for this feature, and we are looking to add it into the roadmap.

- Is Ubitexx agent-based?
  - No, not for now.

- Panic button on PlayBook or Ubitexx?
  - This is also available from a 3rd party solution. It is not built into the standard Ubitexx or PlayBook or BlackBerry feature but can be done at the device level.

- What about Personal Liable?
  - [Ms. Lee provided a long example from one of her clients and two white papers. The example is marked, "Internal Distribution Only," and the Scrivener received the message, "Internet Explorer cannot display the webpage" when he attempted to open the attached white papers.]

- Version 6.0 handheld upgrades can't seem to leapfrog to the newest version without loading each version.
  - [Ms. Lee said she is working on this issue and will follow up soon.]

- [Ms. Lee also provided the following URL: www.blackberry.com/chalk as a starter pack option for testing.

3. Risks and Issues

- No new risks or issues identified.

4. Action Items

- No new action items were identified.

ACRONYMS:

CY2011 = Calendar Year 2011
IT/CIO = Information Technology/Office of the Chief Information Officer
ITSO = Information Technology Security Office
LTE = Long Term Evolution
MDM = Mobile Device Management, Mobile Device Management System
OS = Operating System
Q&A = Questions and Answers
QNX = A Unix-like operating system
RIM = Research in Motion Corporation
TCO = Telecommunications Office
TMO = Technologies Management Office
URL = Uniform Resource Locator

Meeting Minutes

Subject	Mobile Device Management (MDM) Weekly Status Meeting	Date	Wednesday, June 29, 2011
Facilitator	Ken McCathran	Time	9:00 AM
Location	4K045	Scrivener	Ben Llewellyn
Attendees	Udaya Chundury, Ken McCathran, Adeeb Parkar, Barry Sessamen, Hadi Tambal,		
	Kimberly Vines-Weathers, Ben Llewellyn		

Acronyms are listed at the end of these minutes.

1. Draft Policy Document

- Barry noted that Avi Bender removed the guidelines from the draft policy document.
- Barry added a form to the draft policy for people to request devices from the CAT.
- Barry said he would distribute the draft policy to the people who are listed as Invitees to these meetings.
- Barry must take the draft policy to Michael Halls, who will vet it through the Bureau. He noted that Kim Higginbotham will disseminate the policy through the bureau.
- There is some uncertainty as to whether this document will be Bureau policy or CIO policy for the Bureau.
- It was noted that we should add a definition of MDM to this document.
  - Participants are asked to send Barry a good industry definition of MDM.

2. MDM Meeting with TMO

- Ken reported that TMO has more granular requirements for the MDM than Ken expected.
  - TMO requires that the MDM support Windows. This caused some concern in the meeting.
  - It was noted that TMO has evaluation criteria, as we do not.
  - Ben recommended that we develop a requirements document of our own, so we can compare our criteria to those identified by TMO.
    - Ken will write a draft requirements document.
    - Ken will arrange a requirements meeting. LTSO will be invited to send a representative, although it was noted that they might decline the invitation.
- It was noted that TMO has its own laptop inventory, rather than using LTSO's.
  - There was general consensus that we should use multiple MDMs, as well, as no one MDM will meet all needs for both groups.
- Adeeb stated that we cannot develop a security plan until we determine the processes.
- Udaya reported that there is a six-week effort in place to develop mobile secure architecture. He anticipated that MDM would be part of this.
- One of the initiating activities in preparing to distribute mobile devices will be for Kenny Harrison to set up a separate wireless network.

3. RFI/RFP for MDM Testing in the CAT

- Priorities were listed as follows:
  - Policy
  - Infrastructure
  - Requirements
  - Evaluation
  - CAT Demo Setup
  - Application Development Standards

- Barry noted the need to make management aware of the full scope, so they understand the effort is to be more than merely, "buy the device."

- It was suggested that we have subgroups, e.g., determine types of standards.
  - Udaya recommended that the standards group be large, and that it contain interlocking subgroups.
  - There was general consensus that we must bring together people from all Census directorates to compile app development standards.
    - Barry mentioned that he is working with ADCOM to ensure we have "Census apps" rather than "GOVS apps," etc.

- Ken noted that we must engage with ACQ before working with anyone on an RFI/RFP.
  - Roger Rhoads is arranging contact with ACQ.

4. Future Topics

- Adeeb is arranging for a representative of Apollo Systems (a Mobile Iron distributor) to give a demonstration at next week's meeting.

5. Risks and Issues

- No new risks or issues identified.

6. Action Items

- Barry will distribute the draft policy to the people listed as Invitees to these meetings.
- Barry will take the draft policy to Michael Halls, who will vet it through the Bureau.
- Ken will generate a draft requirements document.
- Ken will arrange a requirements meeting, with a special invitation to LTSO to send a representative.

ACRONYMS:

ACQ = Acquisition Division
ADCOM = Associate Director for Communications
CAT = Center for Applied Technology
CIO = Office of the Chief Information Officer
GOVS = Governments Division
LTSO = LAN Technology Support Office
MDM = Mobile Device Management, Mobile Device Management System
RFI = Request for Information
RFQ = Request for Quote
TCO = Telecommunications Office

TMO = Technologies Management Office

Meeting Minutes

Subject	Mobile Device Management (MDM) Weekly Status Meeting	Date	Wednesday, July 6, 2011
Facilitator	Ken McCathran	Time	9:00 AM
Location	4K045	Scrivener	Ben Llewellyn
Attendees	Ken McCathran, Adeeb Parkar, Roger Rhoads, Barry Sessamen, Kimberly Vines-Weathers, Scott Williams, Ben Llewellyn		
Guests from Verizon Wireless	James Briley, Jr., Joel Daniels, Bill Lewis, Mitch Mitchell, Jill Renshaw, Emily Waldron		

Acronyms are listed at the end of these minutes.

1. Guest Speakers

- A cadre of representatives from Verizon Wireless were the guest speakers. They had been invited to discuss their MDM as well as other products and services they currently offer.

- Their presentation focused on a suite of five products, which they said could be used separately or together in any combination:
  - Mobile Services Enablement Platform – Helps generate apps or bridge apps from one device to another
  - Mobile Device Management – Controlling the devices, which apps are allowed/disallowed, security, upgrades and automated setup.
  - Mobile Security – Geofencing, disabling lost devices, speaking through stolen devices, flexible policies set for different needs and services.
  - Inventory and Expense Management – Can be made granular (who used it and when), not just general billing.
  - Logistics – International phone setup, etc.

- The guests suggested several times that Census representatives visit the Verizon office for an executive briefing.
  - If interested, arrangements should be made through Bill Lewis (202-329-5060).

- Verizon has acquired Terremark, which has improved their security capabilities (Verizon has both mobile security and cyber IT security).

- The guests noted that many of their customers use multiple MDM solutions provided by multiple vendors, as no one solution seems able to cover all needs or contingencies at this point.
  - Verizon stated that its product works fully with BlackBerry devices.
  - They stated that, when working with Apple products, their products are the most advanced on the market.
  - They acknowledged having difficulties working with Androids:
    - Not necessarily a technical issue
    - Matter of permissions, open source technology, etc.
  - Census requested a copy of a slide that lists Verizon's capabilities with devices provided by several companies (RIM, Apple, Sprint, etc.).
  - Barry asked for a roadmap of Verizon's goals for gaining which capabilities with what devices, and when.

- There are different ways Verizon's products allow clients to manage devices:
  - Some manage by policy.
  - One client manages according to device (e.g., all BlackBerry devices, all Apples, etc.).

2. Risks and Issues

- No new risks or issues identified.

3. Action Items

- None.

ACRONYMS:

IT = Information Technology
MDM = Mobile Device Management, Mobile Device Management System
RIM = Research in Motion

Gartner Research

Publication Date: 13 April 2011 ID Number: G00211101

Magic Quadrant for Mobile Device Management Software

Phillip Redman, John Girard, Leif-Olof Wallin

As smartphones proliferate in the enterprise, companies are struggling to manage policy, security and support. Enterprise mobile device management software is evolving to offer smartphone (and other device) support across a variety of platforms.

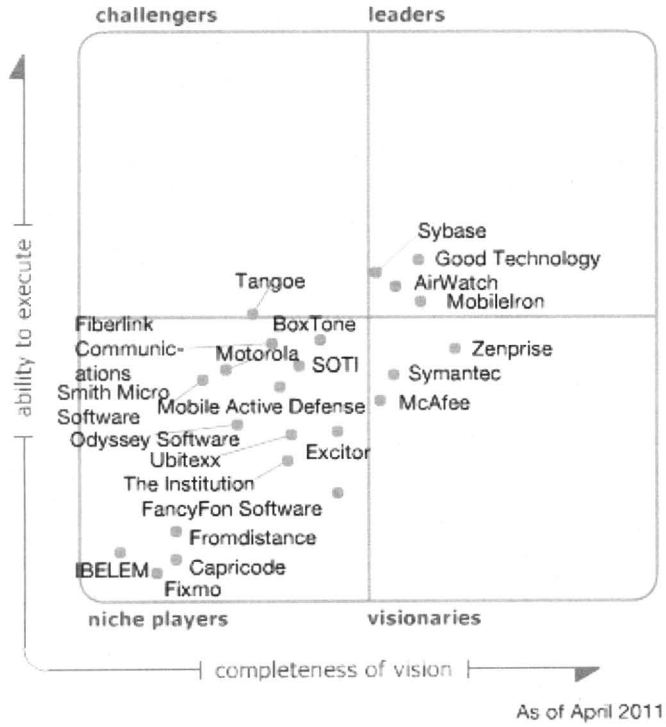
WHAT YOU NEED TO KNOW

This document was revised on 18 April 2011. For more information, see the Corrections page.

Although some of the vendors and products have been around for a long time, mobile device management (MDM) is a nascent market, and the vendors' offerings have little consistency. Many come from mobile messaging and security to support MDM, and, worldwide, there are more than 60 companies in this space. Of these, 42 were deemed potential candidates for this Magic Quadrant (see Figure 1) and were sent questionnaires; 23 met Gartner's inclusion criteria.

MAGIC QUADRANT

Figure 1. Magic Quadrant for Mobile Device Management Software



Market Overview

Introduction

As smartphones and other mobile devices grow in popularity in enterprises, management challenges are beginning to arise — from the cost of the services associated with the devices, to the security and policy that mobile devices should follow. Mobile devices such as smartphones and tablets are increasing in power and memory, and, although they are not replacing PCs on a full-time basis, they are often used as primary communication devices. Also, the number of vendors and platforms in the mobile device market continues to increase and add complexity.

By 3Q10, there were more than 30 global smartphone vendors and more than 10 mobile operating-system platforms, although the top four (Apple, Android, RIM and Symbian) control 89% of the total market. Most adopting companies that had previously standardized on a mobile platform (for example, BlackBerry in North America and Symbian in Western Europe) now need to support multiple operating systems, and Apple and Android have become more popular. However, most organizations don't have anyone responsible for managing mobile devices.

Although procurement may be found in finance or IT, there hasn't been any reason to bother with cellular phones after purchase. However, that's changing. Today, the smartphone is likely to be managed by the messaging group, which is responsible for the BlackBerry Exchange Server (BES), rather than by the entity responsible for managing computing hardware. Although many companies may have device management responsibilities, usually for hardware such as PCs or phones, current software doesn't really cover mobile devices, nor is IT staff trained to support handheld devices.

Elements of MDM

Although many companies are trying to solve a similar problem, it takes multiple types of mobile software to address a full solution. A fully managed mobility solution cuts across standard MDM and telecom expense management and includes:

- **Software Distribution** — The ability to manage and support mobile application including deploy, install, update, delete or block.
- **Policy Management** — Development, control and operations of enterprise mobile policy.
- **Inventory Management** — Beyond basic inventory management, this includes provisioning and support.
- **Security Management** — The enforcement of standard device security, authentication and encryption.
- **Service Management** — Rating of telecom services.

Conclusion

The MDM market is quickly evolving. The requirements and definitions are changing rapidly, and vendor offerings will evolve quickly and be even more capable and mature by next year. High demand is creating a frenzy of development, as well as hope. Although many of the successful MDM providers have focused almost exclusively on mobility, during the next few years, those managing PCs will also be investing and looking for opportunities in the MDM space. Most vendors now offer on-premises or software-as-a-service (SaaS)-based tools, and more-mature managed service offerings will emerge during the next three years to drive growth in the industry.

Some key things to keep in mind when assessing an MDM vendor are:

- Some of the device platforms will limit manageability, due to inherent manufacturer design — don't expect MDM solutions to address each platform the same way or support it the same way.
- Android support is still immature — it will be another year before Android is well-supported by most MDM vendors.
- BlackBerry support is still important — not all MDM vendors support BES integration. It is important that BlackBerry support continues, because, in many regions, it is still the most-supported enterprise device, even as other platforms take away market share.

MDM tools won't beat the BES, but should be able to help manage and report on BlackBerry devices.

- Don't underestimate reporting — for some vendors, their reporting and business intelligence (BI) tools are simple if they have them at all.
- Reporting on device status will be a critical component, and vendor capability to offer both text and graphical reports, canned and customized, is critical.

With the advent of new devices, the MDM market is growing quickly. If we assess pure MDM revenue (excluding revenue for messaging, security, etc.) year-end 2010 is estimated at $150 million, increasing at a compound annual growth rate (CAGR) of 15% to 20% during the next three years.

Market Definition/Description

Enterprise MDM products and services help enterprises manage the transition to a more complex, mobile computing and communications environment by supporting security, service, software and inventory management across multiple operating-system platforms, primarily for handheld devices such as smartphones and tablets. To meet Gartner's definition, MDM vendors must address at least three of the four "elements of MDM" set forth in the market overview and support MDM capabilities or features in mobile application platforms, with an emphasis on MDM. Rated vendors are generally expected to be able to respond competitively with respect to the following features and functions.

Inclusion and Exclusion Criteria

Gartner is aware of more than 60 vendors that claim some level of play in MDM on a global basis. In most markets, even growth markets, large numbers of competing vendors with similar products are cause for concern and indicate a need for competitive natural selection and consolidation.

Inclusion Criteria

After due consideration, 23 vendors were selected to be included for ranking in this Magic Quadrant. The following criteria are necessary for inclusion:

- Support for enterprise-class (noncarrier), multiplatform support MDM: software or SaaS, with an emphasis on mobility
- Specific MDM product focus and feature set or a primary focus on MDM in another product set (messaging or security)
- Security management, with at least these features:
  - Enforced password
  - Device wipe
  - Remote lock
  - Audit trail/logging
  - "Jailbreak" detection
- At least mobile OS 3 platforms supported
- Policy/compliance management

- Software distribution, with at least these capabilities supported:
  - Application downloader
  - Application verification
  - Application update support
  - Application patch support
- Inventory management, with at least these capabilities supported:
  - External memory blocking
  - Configuration change history
- Managing at least 25,000 mobile lines
- Five referenceable accounts
- At least $1 million in MDM-specific revenue

Exclusion Criteria

MDM companies not included in this Magic Quadrant might have been excluded for one or more of these conditions:

- The company did not have a competitive product on the market for a sufficient amount of time during calendar year 2010 and the first quarter of 2011 to establish a visible, competitive position and track record.
- The company had a minimal apparent market share and low market inquiry interest among Gartner clients.
- The company was invited to participate, but did not reply to an annual request for information and did not otherwise meet the inclusion criteria. Alternative means of assessment, particularly client requests and competitive visibility, did not meet the inclusion criteria.

The large number of vendors claiming presence in this market makes it impossible to include every company. Vendors were individually reviewed, discussed and selected by a team of analysts.

Added

This is the first Magic Quadrant published for this market, so all vendors referenced are new to this research.

Dropped

This is the first Magic Quadrant published for this market, so there is no history of vendors dropped.

Evaluation Criteria

Ability to Execute

Gartner analysts evaluate technology providers on the quality and efficacy of the processes, systems, methods or procedures that enable IT provider performance to be competitive, efficient and effective, and to positively affect revenue, retention and reputation (see Table 1). For MDM, this involved providing on-premises-based or SaaS capability with the required number of features to manage the software, security and inventory of a midsize or large (more than 1,000 devices) organization. Although global scaling is important, there should be significant domestic or regional penetration at leading companies.

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product/Service	high
Overall Viability (Business Unit, Financial, Strategy, Organization)	high
Sales Execution/Pricing	standard
Market Responsiveness and Track Record	standard
Marketing Execution	standard
Customer Experience	high
Operations	standard

Source: Gartner (April 2011)

Completeness of Vision

Gartner analysts evaluate technology providers on their ability to convincingly articulate logical statements about current and future market direction, innovation, customer needs and competitive forces, as well as how they map to the Gartner position. Ultimately, technology providers are rated on their understanding of how market forces can be exploited to create opportunity for the provider. MDM providers should have a significant vision (see Table 2) on the evolving market, including software delivery methods, innovative and differentiated features, geographic expansion, as well as distribution and technology partnerships.

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	high
Marketing Strategy	standard
Sales Strategy	no rating
Offering (Product) Strategy	high
Business Model	standard
Vertical/Industry Strategy	no rating
Innovation	high
Geographic Strategy	standard

Source: Gartner (April 2011)

Leaders

Leaders demonstrate balanced progress, effort and clout in all execution and vision categories. If they do not dominate in sales, they are, at a minimum, the most critical competitive threat to their peers in open competition. A leading vendor is not a default choice for all buyers, and clients are warned not to assume that they should buy only from the Leaders quadrant. To stay on the right side of the chart, Leaders (and Visionaries) must offer features that remove significant roadblocks to the complex challenges enterprises face when attempting to treat mobile consumer devices as business tools. One example of a competitively disruptive activity might include delivering a sandbox method to prevent data leakage between personal and business applications.

Challengers

Challengers have attractive products that address the typical baseline needs for MDM with competitive visibility that is strong enough to demand attention in RFPs. Challengers may win contracts by competing on a limited selection of functions or a limited selection of prospect buyers by industry, geography or other limiting factors, even if, on spec, their products have broad functions. They may be perceived as a threat by other vendors, but that threat will be primarily focused on a limited class of buyers, rather than the MDM market as a whole. Challengers are efficient and expedient choices for defined access problems.

Visionaries

Visionaries are able to demonstrate long-term strategies for MDM that point to the product and service approaches that will be most competitive in the future. Visionaries might affect the course of MDM, but they lack the execution influence to outmaneuver Challengers and Leaders. Buyers may pick Visionaries for best-of-breed features, and for broader infrastructure investments than Niche Players. Smaller vendors may take risks on potentially disruptive technologies, while larger vendors may be in the process of building out their next-generation portfolios. Buyers of Visionaries' products may base their selections on specific technology features and by participating in the vendor's road map.

Niche Players

Niche Players meet the typical needs of buyers and fare well when given a chance to compete in a product evaluation. Niche Players generally lack the clout to change the course of the market. They may offer an uncommon delivery mechanism for products and services. They may rely on a self-limiting business model, and/or have limited influence outside of a particular industry or geography. Niche Players may target clients that, for various reasons, prefer not to buy from larger network players. In many Gartner market studies, buyers report that Niche Players tend to provide more personal attention to their needs.

Vendor Strengths and Cautions

AirWatch

Founded in 2003 and based in Atlanta, Georgia, AirWatch emerged from the wireless network management services and ruggedized device market, where management SLAs are critical. AirWatch puts emphasis on device status monitoring and help desk controls. AirWatch support is offered for Android, iPhone, iPad, Nokia S60, full Windows (Panasonic Toughbooks), Windows Mobile, Windows 7 and BlackBerry models.

Strengths

- Options for insourcing and outsourcing of products and services accommodate a wide range of needs, including purchased/insourced systems, SaaS hosted on the user site and SaaS hosted as a cloud service.
- The management console features a strong dashboard and detailed reporting capabilities.
- Multitenant support is designed in for improved scaling, with selective isolation for large installations.
- AirWatch promotes rich policy management in non-Microsoft e-mail server environments, such as any Post Office Protocol (POP)/Internet Message Access Protocol (IMAP)/SMTP mail server, as well as Lotus Domino, Novell GroupWise and Gmail.
- Revenue, while coming from the low end, has been ramping up quickly during the past two years.

Cautions

- Gartner has received feedback from user references regarding poor postsales support.
- The company needs to increase management experience, and is pursuing a plan to hire high-profile managers.
- AirWatch has an international presence, but it still relies on North America for more than 80% of its revenue.

BoxTone

BoxTone, based in Columbia, Maryland, has a large and well-established installed base of BlackBerry devices under management, with a deep understanding of security and enterprise needs and is focused on the mobile market. Although BoxTone continues to strongly support BlackBerry devices, it also supports Android phones, Apple iOS 4 devices and Microsoft smartphone platforms. BoxTone provides deep integration directly with BlackBerry BES, Microsoft Exchange ActiveSync and Good Technologies. It also connects with many popular system management and monitoring platforms (e.g., Microsoft, HP, CA Technologies, IBM and BMC Software). BoxTone provides limited support for HP Palm OS, Nokia S60 and Nokia MeeGo devices. BoxTone mobile service management extends MDM to include service desk management, incident management, problem management and application performance management.

Strengths

- BoxTone's expertise in BlackBerry installations is a plus for RIM facilities, especially large, business-critical mobile deployments and regulated industries.
- The company has strong real-time mobile analytics and enables comprehensive service quality management and policy compliance enforcement.
- BoxTone has executed well with enterprise-class, reliable mobile software, including noteworthy postsales support, high customer-satisfaction rates and repeat business (add-on revenue).

- Unique automated predictive analytics, proactive alerting, real-time diagnostics and problem resolution with embedded best-practice knowledgebase capabilities speed break/fix to reduce downtime.
- The company emphasizes a comprehensive modular mobility management approach spanning multiple IT roles: user self-service, service desk, IT operations, data center operations, security, compliance, applications, finance and IT management.
- BoxTone has an aggressive and competitive MDM street price.

Cautions

- BoxTone's consolidated dashboard with prepackaged report capabilities provides limited customization or requires additional services.
- BoxTone does not require the use of an on-device agent — using a server-based architecture to manage the device, applications and mobile services remotely via native APIs. Although this approach is simple to deploy, it requires a remote agent to be deployed on certain devices for more-complete functionality, which limits the ability of their MDM solution to provide offline and local policy enforcement.
- The text-based user interface (UI) isn't as visually advanced as those of its competitors.

Capricode

Capricode is based in Oulu, Finland. The company started out in 2002 and has remained focused on MDM since 2006. Capricode sells mainly through channel partners in the Nordic countries, and is privately held. The SyncShield Advanced Mobile Device Management product is available as on-premises, SaaS and as a hosted solution from service providers.

Strengths

- Capricode's revenue and installed base is growing rapidly, and the product has had some success with mobile operators as a sales channel for enterprises.
- The solution is delivered completely over-the-air, without user intervention, reducing the challenges during the implementation process.

Cautions

- Capricode is a relatively small company, with limited marketing and operations capabilities, focusing on the Nordic countries.
- The MDM features supported on the different operating-system platforms vary significantly, making it difficult for enterprises to implement a consistent cross-platform policy.
- The product lacks support for RIM OS. A command proxy interface to BES, at a minimum, would be a desirable future capability.

Excitor

Excitor is based in Taastrup (Copenhagen area), Denmark. The company started out in 2001 developing vertical mobile applications in areas such as healthcare. Excitor subsequently started to develop MDM capabilities, initially as part of its DME mobile e-mail solution. The MDM functionality has been further enriched and is now available as a stand-alone product, DME Mobile Device Manager. Most of the installed base has historically been in the Nordics,

predominantly in the financial services vertical, but in the past year, a significant number of clients have been added in the U.S., the U.K., Germany and the Asia/Pacific (APAC) region, as well as across a variety of industries.

Strengths

- Excitor has a reputation for good customer support and strong references.
- Its licensing is based on perpetual licenses, with an additional maintenance charge and with a cloud-based option with per-user, per-month pricing. Pricing is clear and well-articulated.
- It has a relatively large installed base, including a number of large organizations. Customer feedback is generally good.
- Its revenue and installed base are growing rapidly again, following a slowdown during 2009.
- It has strong security, as well as a container approach to separate personal versus corporate data.

Cautions

- International expansion to complement the strong local presence in the Nordics is well under way in the U.K., the U.S., Germany and the APAC region, but in early stages.
- No stand-alone service management capability.

FancyFon Software

FancyFon is based in Cork, Ireland, and also has a presence in Poland. The company was founded in 2006 and is exclusively focused on multiplatform MDM. FancyFon Mobility Center provides a full range of MDM functionality, and is available as an on-premises and a hosted solution. Most of the installed base is in Europe and North America. FancyFon is a privately held company.

Strengths

- It has strong tool capability and platform support, including Android, BlackBerry, iPhone/iPad, Nokia S60, WebOS, Windows Mobile 6.x and Windows Phone 7.
- Its focus is on small or midsize businesses, with an increasing focus on large enterprises.
- Its revenue and installed base are growing rapidly, and the product has had some success with mobile operators.

Cautions

- FancyFon has limited vision and expansion capabilities.
- FancyFon is a small company, with limited operations capabilities outside its strong European presence.
- The MDM features supported on the different operating-system platforms vary significantly, with the strongest support for the Symbian platform.

Fiberlink Communications

Founded in 1991, Fiberlink Communications provides SaaS and managed services for enterprise mobility management. Fiberlink started business in remote access service management, offering a connection agent to negotiate worldwide Internet access for traveling users. The Fiberlink MaaS360 support is offered for Android, BlackBerry, iPhone/iPad, Nokia S60, WebOS, Windows Mobile 6.x and Windows Phone 7 models.

Strengths

- Fiberlink has proven long-term viability and global presence, with most revenue originating in North America and Europe.
- The Fiberlink management MaaS360 client agent and user self-service portal are already known and visible in the remote access and virtual private network (VPN) market frames of reference.
- The company is experienced in mobility and telecom services delivered through scalable cloud-based network operations centers (NOCs). Fiberlink offers good mobile analytic tools and device status reporting.
- The customer base is spread across industries that are growth targets for mobile access.
- MaaS360 enables iPhone/iPad users to subscribe to enterprise document and database updates through the Apple enterprise application distribution function.

Cautions

- The company has had a long, but historically weak, competitively recognized role in delivering SaaS and point services for PCs starting in the early 1990s and for PDAs starting in the late 1990s. The company has not generated broad competitive recognition of MDM capability, despite past attempts to break free of its historical network management service provider roots.
- Fiberlink has low visibility in MDM — it needs increased investment in sales and marketing.
- MDM SaaS is not yet widely popular, although Gartner anticipates rising interest as cloud service adoption increases.

Fixmo

During the preparation of this research, Fixmo, a Toronto, Canada-based company, announced its intent to acquire Conceivium Business Solutions, a vendor that had already qualified for inclusion in this Magic Quadrant. The acquisition was completed before this research was published. The name has been changed in this research to reflect the new owner and brand. Founded in 2004 and based in Virginia, Conceivium began as a value-added management provider for BlackBerry environments and has added support for Apple and Android devices. The business model relies primarily on resellers to implement and maintain the technology. Conceivium MobileAnalyzer/MobileMonitor support is offered for Android, BlackBerry and iPhone/iPad models. Fixmo is also looking to add some capabilities using the Odyssey platform, and it has recently entered into an agreement to incorporate Good Technology.

Strengths

- Conceivium's MobileAnalyzer makes an attractive account-monitoring platform and is used by several large, traditional, managed infrastructure service providers. For example, it can integrate with HP OpenView and IBM Tivoli. There is a logical opportunity to expand into offering telecom expense management services.
- E-mail support includes Microsoft Exchange, Lotus Notes and Novell GroupWise.
- A partnership with Good Technology will help expand support on new phone platforms and provide an opportunity to associate with a better-known brand. However, any connection with so strong a competitor in the same market will cannibalize opportunities.
- Fixmo will bring a larger employee base, more funds and a compatible mobile monitoring business into the picture.

Cautions

- Conceivium historically relied on the BlackBerry market and has limited application and policy management on iPhone/iPad and Android platforms, which will expand when combined with Fixmo Sentinel in the future.
- Prior to the acquisition, Conceivium claimed a relatively large number of managed end points, but not a revenue base to explain it. Small revenue; lack of a presence outside North America; relatively slow, but steady, growth; and a critically small employee base factored strongly in setting Fixmo's execution and vision ratings.
- The Fixmo acquisition resolves the immediate questions of viability, but, otherwise, does not change the ranking decisions afforded to Conceivium in this research. The new company's market performance will be re-evaluated for the 2012 Magic Quadrant.

Fromdistance

Fromdistance is based in Tallinn, Estonia, and was founded in 2004. The company is private, with venture funding. Most of the client base and distribution partners are located in the Nordic countries. The MDM product is available for RIM OS, Symbian, Apple iOS, Android and Windows 6.x. The product also has capabilities to manage Windows CE/XP/Vista/7 clients.

Strengths

- Fromdistance revenue and installed base is growing rapidly, and the product has had some success with smartphone distributors, operators and service providers.
- It has versatile server capabilities. One of the few hosted MDM solutions, the product is available as on-premises, SaaS and as a hosted solution from service providers.

Cautions

- Fromdistance is a small company with limited marketing and operations capabilities, with a strong local, Nordic focus.
- It has little visibility among medium and large companies as an MDM vendor.

Good Technology

Good Technology, based in Redwood Shores, California, has a long history in the mobile applications space and thousands of clients globally through its e-mail system, which garnered

strong sales as a NOC-based architectural alternative to BlackBerry Enterprise Server for non-BlackBerry mobile shops. Lack of hardware hampered its sales, and, during the past two years, new ownership and senior leaders have repositioned it as an MDM platform. Focusing on security, it has seen success with financial services, government, healthcare, legal, professional services and other security-conscious enterprises. Though Good does not have a separate MDM product and supports MDM as a feature of its Good for Enterprise solution for secure messaging and intranet access, it is included in the Magic Quadrant, because it supports the criterion, it is purchased specifically for MDM and it is highly requested as an MDM product through inquiry.

Strengths

- Has the best name recognition in MDM and appears frequently on shortlists, although the company's primary product is secure e-mail.
- Good's mobile security features, particularly platform-independent FIPS 140-2 encryption in the e-mail system, have helped to catalyze entry for Apple devices into organizations bound to stringent data protection requirements.
- Good can validate and authorize specific applications before allowing them to connect to a corporate network. This feature is available even on platforms that do not support blacklisting and whitelisting, such as iPhone and iPad.
- Good has a track record for supporting and managing both corporate and personal data and applications and is compatible with both Microsoft Exchange and Lotus Notes
- Extensive help desk features are included, as well as a user self-service portal.

Cautions

- Users must deploy Good for Enterprise Server and transmit end-to-end encrypted data through Good's NOC.
- Strongest security for messaging and Intranet access through the Good client and its FIPS 140-2 certified encryption; otherwise, it uses native encryption or must use third-party applications for non-Good applications.
- Good provides its own UI for corporate e-mail and personal information manager access. In many cases, this causes complaints from users, who must be convinced of the benefits of the added security in exchange for the UI replacement.
- The cost of the Good solution can be relatively high per user seat, compared with other vendors. Furthermore, the installation and configuration of advanced security features are complex and require a learning curve.
- Good does not offer management or integration for BlackBerry.

IBELEM

IBELEM is based in Nanterre, France, and also have a development team in Nantes, France. IBELEM was founded in 2001 and was initially focused as an SI for mobile applications. Since 2008, IBELEM has developed its own MDM capabilities. The PushManager product is provided as an on-premises or SaaS solution. The installed base is almost exclusively in France. IBELEM is a private company, with venture capital (VC) funding. The MDM product is available for BlackBerry, Symbian, Apple iOS, Android, Windows Phone 7 and Windows 6.x.

Strengths

- Licensing is based on a perpetual license plus maintenance or a per-device fee for SaaS. Pricing is clear, and enables clients to start small and grow over time.
- The installed base consists of a mix of small and relatively large clients.

Cautions

- IBELEM is a small company, with limited operations capabilities and a strong French focus.
- The MDM features supported on the different operating-system platforms vary somewhat, and the on-premises and SaaS solution for the same platform also vary; RIM OS is not supported.
- IBELEM marketing and awareness remains weak outside France.

McAfee

Based in Santa Clara, California, McAfee is a prominent global security player with strong positions in desktop and laptop antivirus, encryption, and comprehensive endpoint management. McAfee entered the MDM realm through the 2010 acquisition of Trust Digital. McAfee EMM support is offered for Android, iPhone/iPad, Nokia S60, WebOS, Windows Mobile 6.x and Windows Phone 7 models. McAfee is not a pure-play MDM, and its focus on broader security solutions, although strategic, does not immediately raise its competitive standing against established MDM players. However, the acquisition posed no product or history conflicts within McAfee product lines, and Trust Digital had already started to develop a reputation for iPhone security at the time of the acquisition. Starting in January 2011, AT&T is reselling EMM as on-premises software.

Strengths

- McAfee EMM offers MDM managed through its broader ePolicy security suite and is extending interoperability out to their larger product portfolio.
- EMM has a strong dashboard and reporting tools.
- Management is compatible with Exchange, Lotus Notes, Groupwise and Gmail
- McAfee has a track record of selling new incremental management products and features into its large, global ePolicy Orchestrator (EPO) installed base. Success in the adjacent mobile data protection market is a noteworthy case in point.
- Revenue and competitive presence for MDM are 60% in North America, with the balance divided mostly between Europe and the APAC region.

Cautions

- In the year since the Trust Digital acquisition, integration of EMM into the McAfee framework has been slower than expected, even if allowances are made for its unexpected acquisition by Intel.
- The UI isn't as sleek as some other competitors, and is less easy to use and navigate.

- EMM is not able to automatically whitelist/blacklist and protect the device if it falls out of compliance, although it can be blocked from further contact using McAfee's Network Access Control (NAC) policies.
- External media encryption is offered for iPad, but not for other at-risk platforms, such as Symbian and Android.
- Pricing per seat is comparatively high, sometimes twice that of its competitors, which reflects a PC valuation mind-set.

Mobile Active Defense

Mobile Application Development Partners, the company behind the service Mobile Active Defense (MAD) is based in Atlanta, Georgia. The company was founded in 2009, and is privately held. Mobile Enterprise Compliance and Security Server is a clientless, zero-footprint MDM product available as an on-premises as well as a hosted solution. Most of the installed base is in North America and dominated by companies and organizations in regulated verticals, such as healthcare or financial services.

Strengths

- MAD employs a novel, strong security approach, using a VPN and a data container. The lightweight design appeals to companies looking for minimal device support burdens.
- The proffered MDM features are uniformly available across the supported platforms.
- The agentless approach supports rapid deployments and may appeal to companies with limited time and/or funds that are in a hurry to implement a basic device-monitoring solution. It has an agent for non-iOS platforms.

Cautions

- Although it has experienced strong initial growth, MAD still has low visibility in the MDM market.
- MAD has not yet developed strong operator or significant channel partner relationships to broaden its growth portfolio, and has seen slower growth than its competitors.
- An agent-based solution provides more control and deeper monitoring of mobile devices. To remain competitive in this market as it matures, MAD should consider a timeline to offer on-device agents.

MobileIron

MobileIron, based in Mountain View, California, launched its product in September of 2009 and has seen rapid growth in sales, mind share and market share, outselling most MDM platforms during the past year. Built from the ground up, it is solely focused on mobility management. Still a startup, it has practices found at more-mature companies, including strong presales and postsales groups. Although primarily focused on North America, we are seeing expansion into a significant presence in Western Europe as well.

Strengths

- MobileIron has rapidly earned high levels of mind share in the MDM market, and appears frequently on shortlists. With strong marketing capabilities, the company has the ability to convey the business value of MDM.

- Strong presales and postsales support and programs are particularly effective at building client relationships and reinforcing credibility.
- The company emphasizes comprehensive life cycle management, including usage monitoring, cost control, and application deployment and version control. It offers strong support for corporate and personal devices.
- MobileIron has a sleek UI and a full-featured tool.
- The product has great reporting and dashboard capabilities.

Cautions

- Being a small startup company, MobileIron could struggle with scaling, especially globally, as a result of early successful growth. It is a good potential acquisition target for a larger vendor that wants to acquire a superior management interface.
- It does not have its own encryption capabilities, must work with what's on-device or through partners, which could cause higher costs. Buyers need to understand the limits of embedded protections on each platform, because these will be the limits to what MobileIron can manage.
- MobileIron offers a physical or virtual appliance, but is not releasing a SaaS offering until 2Q11.

Motorola

Based out of the newly formed Motorola Solutions in Illinois, the MDM portfolio consists of the Motorola Mobile Services Platform (MSP), originally designed to support its full line of ruggedized Windows-based mobile devices, including Windows Mobile 6.x. Recently, it has been expanded to support Apple and Android. RIM support is planned for future release this year. Motorola has seen good adoption in the ruggedized world, but is less known and has a smaller market share in non-Motorola and smartphone devices.

Strengths

- It has strong support for Motorola ruggedized devices and peripherals.
- It is available as software for internal operations or as a managed service.
- Motorola offers a vendor-agnostic open system, with integration to corporate management platforms, such as HP OpenView and IBM Tivoli.
- Motorola has proven global scale and support for its MDM offering.

Cautions

- Motorola has emerging horizontal smartphone experience, but has been more focused on ruggedized devices.
- It is little known in the horizontal enterprise market.
- It has limited distribution channels beyond industrial space.

Odyssey Software

Founded in 1996, Odyssey Software, based in West Henrietta, New York, started off by managing ruggedized handheld devices. It is engaged in distribution and license agreements with other companies in the MDM market, including AirWatch, Good Technology, Motorola and Symantec, as well as marketing and developer partnerships with several mobile device platform vendors and mobile operators, including Microsoft, Samsung, LG, Motorola, HTC, RIM, Apple, AT&T and Verizon.

Strengths

- Odyssey's sales are primarily in North America, it has a growing presence in all world markets.
- Long-term MDM experience and execution are assets — seat sales have been growing at a reported rapid rate of 37% CAGR during the past seven years, primarily through licensees.
- Odyssey has full-featured software and inventory functionality across multiple platforms, with support for platform-specific security.
- The company provides unique device support via integration with Microsoft System Center.

Cautions

- Odyssey's practice of increasingly licensing products and technologies to other vendors in the same market reduces direct sales revenue potential and cannibalizes opportunities to compete in RFPs.
- Despite a long time in the MDM market, Odyssey has less visibility in open competition, due to its direct sales focus on Microsoft System Center customers and not being a commonly referenced brand outside that association. This weakness weighed strongly on its ranking.

Smith Micro Software

Smith Micro, based in Aliso Viejo, California, works with many Tier 1 wireless operator selling its connectivity solutions and is engaged with all major wireless OEMs to support new device launches on behalf of those wireless operators. In addition, Smith Micro has a commercial relationship with HTC and supplies its standards-based OMA-DM MDM client for its Android handsets shipping to North America, and Asian markets. Smith Micro sells MDM support for iOS, Symbian and Android to the enterprise market through its direct sales force and is actively recruiting indirect channel partners, including value-added resellers, system integrators (SIs) and service providers.

Strengths

- Smith Micro has a strong and experienced software development group.
- It has good carrier partners and relationships.
- It provides broad mobile operating-system platform support.

Cautions

- Smith Micro has a weak direct enterprise sales and support channel.

- It has no service management capabilities.

SOTI

Based in Mississauga, Ontario, Canada, SOTI has a long and successful background in supporting ruggedized handhelds based on different Microsoft operating systems Recently, support has been added for Apple and Android in its core MDM product MobiControl. SOTI has been successful in vertical industries deploying ruggedized devices, but is less known and has smaller market share in the generic smartphone market.

Strengths

- It has strong support for ruggedized devices and peripherals.
- It is available as software for internal operations or as a managed service.
- SOTI has a global presence through partners and good support capabilities.
- It offers a strong tool capability with a good UI and multiple methods of use.

Cautions

- Generic smartphone support has only recently been launched.
- It is unknown outside industrial uses.
- Good customization on the dashboard and reporting views, but no overall graphics on it.

Sybase

Sybase, an SAP company, is based in Dublin, California. It owns the longest-established MDM platforms, reaching back to PCs in the late 1980s. Afaria was created in 1997 for laptops and subsequently released in 2000 as the first nonindustrial MDM platform for Palm and Windows devices. Afaria support is offered for Android, BlackBerry, iPhone/iPad, Nokia S60, Windows Mobile 6.x and any phone model that supports Open Mobile Alliance (OMA) Device Management (DM). Afaria also has value-added mobile features for tablets running Windows 7.

Strengths

- Afaria offers broad life cycle management benefits and, when combined with Mobile Office, constitutes a comprehensive wireless e-mail and mobile application integration framework. It constitutes the most mature platform among MDM vendors for managed software distribution.
- Feature sets for help desk support, application and service management, including expense management, are well-represented across the most popular smartphone platforms. Noncompliant devices can be quarantined.
- Sybase is one of a few MDM vendors that offers an embedded VPN in its e-mail client, plus a sandbox facility to isolate and control application access to business data and VPN connections.
- Afaria offers support for an Android application portal for enterprise application management. Afaria Advanced Enterprise Security (AES) for Android, adds more than 80 device management features on Samsung Android devices.

Cautions

- Afaria can be relatively expensive per user seat (twice that of competitors); but this is also true of other vendors with broad functional platforms. To use features such as e-mail encryption, buyers may need to invest in Mobile Office, in addition to Afaria.
- Feedback to Gartner indicates that buyers find the installation of Afaria to be complex. Companies planning a new/first purchase must plan for a learning curve.
- The Afaria UI has been on the market for some time and needs an update.

Symantec

Symantec is a prominent global security player, with strong positions in desktop and laptop antivirus, encryption and comprehensive endpoint management. Symantec has offered MDM support in Altiris since 2004. Symantec SMM support is offered for Android, BlackBerry, iPhone/iPad, Nokia S60, WebOS, Windows Mobile 6.x and Windows Phone 7. Although Symantec has had MDM for years, Gartner analysts have not seen evidence of competitive public visibility until recently, and cannot verify a significant presence through client references. Symantec has successfully obtained all the pieces for a strong MDM platform; however, its strong focus on security causes a diminution of understanding of the business and operational requirements for mobile device life cycle management. Support for security policy management is strong and complete across the widest range of mobile platforms; however, support for nonsecurity functions is patchy.

Strengths

- Symantec SMM provides strong security capability with lightweight client options. Integration with other Symantec product frameworks is a strategic advantage for long-term Symantec customers.
- Symantec is emphasizing advanced iOS and Android features, such as elective e-mail data wipes, full e-mail access control, selective wipe on application data, hardware asset tracking, selective whitelist/blacklist and application management, as well as data-roaming policies.
- Symantec has an outstanding track record for overall viability and for competitive sales and support of a wide range of security services. Their global reseller network is strong and well-trained.
- Symantec offers an industry-leading central policy management system for endpoint devices.

Cautions

- The MDM console isn't as attractive or user-friendly as competitors' and could use updating. Although it provides life cycle management, the console emphasizes a focus on security.
- Buyers who want to build a complete MDM solution may require additional Symantec product lines, especially to complete the security functions.

Tangoe

Tangoe is a fast-growing TEM company based in Orange, Connecticut, with 2010 estimated sales expected to grow to approximately $85 million. Though the primary revenue source is

through TEM, it also has seen the adoption of its MDM platform, acquired from Internoded, also grow in the past 18 months. It has done a good job at integrating TEM and MDM, as well as offering MDM as a service, although full maturity has not yet arrived.

Strengths

- Tangoe is a well-known company in the TEM services market. It can directly leverage its credibility with enterprise IT operations to compete for MDM service fulfillment.
- Tangoe provides consistent life cycle management capabilities across supported platforms.
- It has long-term experience at provisioning and tracking mobile devices on all known platforms.
- When combined with TEM services, Tangoe's MDM pricing is aggressive, inexpensive and highly competitive.

Cautions

- The management and client interfaces are basic design and appearance and need an update.
- The tool offers little beyond the standard reporting functions, and it needs to provide deeper capabilities.
- Although Tangoe has increased its global reach, primarily through its TEM service, its primary focus has been on North America for MDM.

The Institution

The Institution is based in Stockholm, Sweden. The company was founded in 2006, and has exclusively focused on MDM since its inception. The Institution provides the product Revival as an on-premises, hosted or SaaS solution. The installed base is almost exclusively in the Nordic region, and is dominated by channel partner sales. The Institution is privately held.

Strengths

- Licensing is based on a per-month, per-device fee, plus initial install and training fees. Pricing is clear and enables clients to start small and grow over time.
- The installed base and revenue are growing rapidly and consist of a mix of small and relatively large clients.
- Customer feedback is generally good.

Cautions

- The Institution is a small company with limited operations capabilities and a strong Nordic focus.
- The Institution marketing remains weak, and has little mind share beyond the Nordic region.
- The MDM features supported on the different operating-system platforms vary significantly, and the RIM OS isn't supported at all.

Ubitexx

Ubitexx is based in Munich, Germany, and has a development center in Kharkov, Ukraine. The company was founded in 2002, initially as a consulting company assisting clients mobilizing their workforces. In 2005, Ubitexx began to develop its own management and security product, Ubi-Suite, which became the exclusive focus for Ubitexx as of 2008. The Ubi-Suite product is provided as an on-premises, hosted or SaaS solution. The installed base is almost exclusively in the Germany, Austria and Switzerland region. Ubitexx is a private company with VC funding.

Strengths

- Ubitexx has strong local support and presence.
- It offers a full-featured tool that can be customized.
- Its licensing is based on a per-month, per-device fee. Pricing is clear and enables clients to start small and grow over time.
- The installed base is growing rapidly, and consists of a mix of small and relatively large clients.
- Customer feedback is generally good.

Cautions

- It has a weak UI and navigation.
- It offers weak reporting and BI capabilities.
- Ubitexx is a relatively small company, with limited operations capabilities and a strong German focus. Ubitexx marketing and awareness remains weak outside Germany.
- The MDM features supported on the different operating-system platforms vary somewhat, and RIM OS nor Windows Phone 7 are supported.

Zenprise

Zenprise was founded in 2003 and is based in Fremont, California. It is a small company focused solely on MDM. It recently acquired a small French security and MDM company, Sparus, to better support mobile security and encryption. It is one of the few vendors with support for WebOS and Windows Phone 7, among the other routinely supported platforms. It has a full feature set for life cycle management for corporate and personal devices. Features include capabilities for help desk support, application deployment and versioning, and cost control through usage monitoring. It offers innovation in areas that other vendors haven't provided yet, including content filtering and automated defense capabilities.

Strengths

- Zenprise has a strong tool UI and functionality.
- It provides end-to-end security via an embedded VPN and sandbox that can control and encrypt application traffic.
- It enables Web content filtering and URL filtering on mobile devices, which differentiates Zenprise from its competitors.

- The product can quarantine noncompliant devices based on policies, devices, operating-system versions, and compliance violations (e.g., user installed blacklisted applications, user "jail broke" the phone, user hasn't upgraded the operating system that addresses security vulnerability).
- Zenprise has a large, installed MDM customer base.

Cautions

- Fair execution and postsales support were reported in our survey; however, marketing is weak, and competitive visibility reported by Gartner clients is low.
- The tool offers weak dashboard and reporting capabilities for supported devices.

RECOMMENDED READING

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

"Magic Quadrants and MarketScopes: How Gartner Evaluates Vendors Within a Market"

"Market Share: Mobile Communication Devices by Region and Country, 3Q10"

"Findings: Consumerization Is Affecting Enterprise Mobility Strategies"

"Mobile Device Management 2010: A Crowd of Vendors Pursue Consumer Devices in the Enterprise"

"Use Managed Diversity to Support Endpoint Devices"

Note 1
The MDM Market

A number of vendors assessed for this Magic Quadrant were not included, because they did not meet our criteria; however, many of them offer some type of MDM software or services. Examples include:

- Absolute Software
- AetherPal
- Avoceen
- CA Technologies
- Cloud Systems
- CommSolv
- CommonTime
- HP
- IBM
- Innopath
- iPASS

- Jamf
- Juniper
- LANDesk
- LRW
- mFormation
- Mobiquant
- Notify
- Novell
- Perlego
- Proximity
- SynchPoint
- Trellia
- Wavelink
- Zelog

Note 2
Supporting Apple iOS Devices

Questions about support for Apple iOS devices continues to grow. Apple controls much of how applications are developed and supported in the enterprise, with no exceptions. Although Apple has increased its enterprise capability, it still has the strictest requirements for enterprise application support. To use MDM capabilities built into iOS 4, your organization must enroll in the iOS Developer Enterprise Program (iDEP). Once accepted, an organization will receive an Apple Push Notification Service (APNS) certificate, which it can load into an MDM platform. This will allow an organization to create, sign and host its own iOS applications, without having to go through the iTunes store. If you are only implementing Simple Certificate Enrollment Protocol (SCEP), then iDEP is not required. An MDM platform is needed to support applications on an iPhone or iPad. Apple publishes a list of its major partners; however, other vendors may also support iOS devices.

All MDM providers use the same method for managing iOS devices, an XML document called the configuration profile, which Apple defines. Because of this, all MDM providers will provide similar features. There are limits, imposed by Apple, to the configuration profile-based management versus other operating-system platforms, which may include:

- Apple has removed the APIs to detect jailbroken phones.
- The root configuration profile can be removed by the user.
- Applications cannot be pushed or pulled onto the device by IT administrators.
- Device may be erased using iTunes and use iTunes for backup.

- Over-the-air operating-system updates are not supported — these need to be done in iTunes.

Vendors Added or Dropped

We review and adjust our inclusion criteria for Magic Quadrants and MarketScopes as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant or MarketScope may change over time. A vendor appearing in a Magic Quadrant or MarketScope one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. This may be a reflection of a change in the market and, therefore, changed evaluation criteria, or a change of focus by a vendor.

Evaluation Criteria Definitions

Ability to Execute

Product/Service: Core goods and services offered by the vendor that compete in/serve the defined market. This includes current product/service capabilities, quality, feature sets and skills, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

Overall Viability (Business Unit, Financial, Strategy, Organization): Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor's capabilities in all pre-sales activities and the structure that supports them. This includes deal management, pricing and negotiation, pre-sales support and the overall effectiveness of the sales channel.

Market Responsiveness and Track Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word-of-mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509