January 3, 2012

Market Overview: Cloud-Hosted Mobile Device Management Solutions And Managed Services

by Benjamin Gray and Christian Kane
for Infrastructure & Operations Professionals
January 3, 2012

Market Overview: Cloud-Hosted Mobile Device Management Solutions And Managed Services
Support Empowered Workers Better By Managing Your Enterprise Mobility Strategy Efficiently And Securely

by Benjamin Gray and Christian Kane
with Doug Washburn, Laura Koetzle, and Alex Crumb

EXECUTIVE SUMMARY
To implement your enterprise mobile strategy, IT infrastructure and operations (I&O) professionals must invest in a mobile device management (MDM) solution. This essential technology allows I&O professionals to support multiple platforms and form factors, extend management and security policies to both corporate-liable and employee-owned devices, and automate service desk support. This is especially important as I&O develops bring-your-own-device (BYOD) programs to support the business needs and high expectations of its empowered workers. So what’s the catch? The MDM market is burgeoning with more than 40 vendors offering on-premises and cloud-hosted solutions. This report is part of a series to help I&O professionals understand the MDM vendor landscape and develop a short list of vendor solutions for further evaluation. In particular, this report evaluates vendors offering cloud-hosted MDM solutions and managed services.

TABLE OF CONTENTS
2 Meeting Today’s Business Demands Requires A Multiplatform Mobile Strategy
3 The Key Criteria That Makes Up Leading Mobile Device Management Solutions
   Core Mobile Device Management Criteria: Configuration, Reporting, And Support
   Mobile Security Management: PIN Enforcement, Data Wipes, Detection, And Encryption
   Mobile Application Management: Software Distribution, Lists, And App Stores
   Differentiating Criteria: Platform Support, Integration, And Availability
12 Segmenting The Market: Innovators, New Entrants, Best-Of-Breed, And Services

NOTES & RESOURCES
Forrester interviewed 24 vendor companies, including AirWatch, Fiberlink, Good Technology, MobileIron, RIM, Sybase, Virtela, and Zenprise, and 184 user companies.

Related Research Documents
“10 Lessons Learned From Early Adopters Of Mobile Device Management Solutions” September 16, 2011


MEETING TODAY'S BUSINESS DEMANDS REQUIRES A MULTIPLATFORM MOBILE STRATEGY

Today’s IT infrastructure and operations (I&O) professionals support an increasingly decentralized and mobile workforce — one with multiple user segments, each with its own unique set of requirements. This poses two significant challenges: 1) their needs often conflict with existing sourcing and support policies, and 2) the applications and devices that workers request are increasingly consumer-centric. This is driving I&O professionals to revisit their mobile strategies to incorporate evolving workforce requirements, and more firms than ever are embracing their empowered mobile workforces.

Forrester encourages I&O professionals to map technology provisioning to user requirements to enable their various user segments to be successful. Firms should start by embracing a leading mobile device management (MDM) solution that supports a wide spectrum of devices and platforms. Here’s why this is so important:

• Approximately half of firms have already embraced a multiplatform mobile strategy. The marriage of BlackBerry devices plus the BlackBerry Enterprise Server (BES) is — and will remain — the gold standard with regard to device management and security, with more than 550 policies for I&O professionals to wirelessly configure and enforce. According to Forrester’s recent survey of 1,051 mobile technologies and services decision-makers, 66% of North American and European companies support BlackBerry today. Despite this leadership, 37% support iOS (the OS that powers both the iPhone and the iPad) and 24% support Android. When asked about their plans over the next 12 months, 84% anticipate continued support for BlackBerry, 83% will support iOS, 77% will support Android, and 61% anticipate also supporting Windows Phone 7.

• Almost 60% of firms provide some support to employee-owned smartphones. As I&O professionals introduce flexibility into the OSes they support, sourcing and vendor management professionals are following suit and loosening their procurement and reimbursement policies. In fact, 59% of firms now officially support personally owned smartphones to some extent which can achieve financial and user satisfaction objectives simultaneously. On one hand, your C-level executives will like the cost savings benefits from personally owned devices. On the other, it will help retain and attract top job talent — especially those empowered workers who want and expect to use the devices they’re comfortable with to be productive. Of course, what classifies as “support” will forever remain in a state of flux as more I&O professionals encourage their workers to self-provision and support each other.

• I&O struggles to keep pace with a twofold challenge: device management and security. Mobility at the enterprise level brings together many traditionally siloed roles within IT, including telecom, end user computing, service desk, security and risk (S&R) management, application development, and sourcing and vendor management professionals. But because MDM and mobile security have traditionally been the responsibility of separate roles — I&O
and S&R, respectively — mismatched policies can easily lead to data security breaches and operational inefficiencies. These often result from miscommunication or the lack of a management solution that serves as a single pane of glass into the current state of the mobile environment.

- **I&O professionals are investing heavily in MDM solutions and managed services.** According to Forrester’s recent Network And Telecommunications Survey, 31% of firms have implemented a MDM solution and another 42% of firms are interested in doing so. Adding support for non-BlackBerry devices — such as the iPhone, the iPad, and Android-based smartphones and tablets — and employee-owned devices has led many I&O professionals to explore third-party MDM solutions that can coexist peacefully with the BES or potentially replace it. Moreover, it’s difficult to find I&O staff who are completely up to speed on the latest devices, OSes, applications, and security threats.

Firms now have a choice between investing in on-premises or cloud-hosted solutions and managed services. Forrester finds that the latter have proven increasingly compelling for firms that lack internal expertise, budget, or that have determined that managing an on-premises solution takes too long to deploy and configure or simply isn't strategic enough for internal I&O professionals to take on. Regardless of deployment model, by embracing these solutions today, firms can set down the path of becoming device-independent with iOS and Android support while also leaving room for emerging platforms such as Windows Phone 7.

**THE KEY CRITERIA THAT MAKES UP LEADING MOBILE DEVICE MANAGEMENT SOLUTIONS**

The pace at which MDM solutions are evolving is dizzying. While last year’s solutions were mostly differentiated by the platforms they support, today, vendors are differentiated around an expanding list of new capabilities centered on real-time reporting, contextual policies, security and application management, and their deployment architectures. Although the majority of deployments is still on-premises solutions, Forrester clients have shown a steadily increasing interest in cloud-hosted and managed mobility services over the last eight months. Fueled by flat or decreasing budgets, firms are finding that the infrastructure, maintenance, and people costs to keep up with this changing market are not sustainable. A never-ending release cycle for mobile OS updates and MDM solutions is influencing these firms to let a vendor handle the solution maintenance so I&O staff can focus on enabling the workforce and protecting corporate data.

**Core Mobile Device Management Criteria: Configuration, Reporting, And Support**

The proliferation of mobile devices is making I&O professionals wary of having to increase staffing to properly support business demand. To stay ahead of the curve, MDM vendors are evolving their configuration, reporting, and support functionality to keep costs down and allow IT support to shift from reactive to proactive. Forrester recommends that I&O professionals prioritize the following core MDM criteria (see Figure 1):
• **Over-the-air (OTA) configuration.** Configuration management tools aid in the administration and control of device settings. I&O professionals can dictate different security, application, and configuration policies for different workforce segments. OTA configuration allows IT to manage devices, regardless of their location.

• **Intelligence, troubleshooting, and support.** Scheduled or event-based actions and real-time monitoring, logging, and web reports all help enable service desk staff to better manage their mobile environments. In some instances, they can help IT identify issues before users even notice.

• **Real-time inventory.** Real-time information on system configuration, installed applications, and security configuration allows MDM policy engines to find compliance issues and perform remediation in real time. This automation eliminates the period of device noncompliance between time of alert and action and frees up I&O staff’s time.

• **Remote control.** Unfortunately, too many help desk requests are PEBKAC (“problem exists between keyboard and chair”) in nature. Regardless of the issue, however, I&O professionals can be much more efficient at troubleshooting tickets when they use remote control to take over the device and experience what the user sees in real time.

• **Self-service portal.** Optimizing IT-to-device staffing ratios is difficult and is made even more so by moving away from a one-size-fits-all approach. I&O can effectively reduce operational costs by enabling a self-service portal for employees to access whenever they have a request. Here employees can review their mobile and expense policies, request software, and back up and restore their devices.

• **Advanced monitoring and actionable alerts.** Each firm has its own unique environment and set of requirements for monitoring device compliance and usage. The ability to create customizable alerts gives IT immediate access to the information it needs to know.

• **Report templates.** New devices, applications, and usage trends mean I&O professionals need to deliver on an entirely new set of reports. Report templates provide IT with a launching point to create custom reports for the ever-increasing number of roles that enterprise mobility touches from application development to security and risk to sourcing and vendor management.
Mobile Security Management: PIN Enforcement, Data Wipes, Detection, And Encryption

Security is becoming an increasing concern as I&O professionals are expected to support a greater number of devices types and mobile platforms. This is particular true when it comes to iOS and Android as I&O professionals feel the pressure to adopt these newer and more consumer devices. MDM vendors are bridging the gap between native device capabilities and IT requirements with these key security technologies. Forrester advocates that I&O professionals prioritize the following mobile security management criteria (see Figure 2):
- **PIN enforcement.** Enforcing a strong password policy — such as PINs and passwords that cannot be brute-force attacked by pulling from a dictionary — is the first and most effective step in preventing unwanted access to a device.

- **Selective data wipe.** The ability to wipe only corporate data from a device while leaving personal data intact is a requirement for any firm considering a BYOD program.

- **Jailbreak/root detection.** Jailbreaking (on iOS) and rooting (on Android) is a means to bypass the management on the device and remove IT control. The ability to detect this on a device and remove its access to the network and corporate assets is a fundamental security need for firms that support these platforms.

- **Data encryption.** Organizations that handle sensitive data may require data-at-rest encryption. iOS has built-in encryption capabilities, both at the device and the file level. A mobile security product can enable the encryption feature on iOS. Android, however, does not have OS-level support for encryption; the mobile security product may have to, or at a minimum, ensure that.

- **VPN.** A secured connection is often a requirement when connecting a device to a specific corporate application or asset. Integration with existing VPN solutions and the ability to manage certificates are requisites that many IT departments require from an MDM provider.

- **Data leak prevention (DLP).** Because mobile devices are increasingly used to process confidential data, organizations are concerned about the risk of inadvertent and deliberate data leaks. DLP is different from data protection functions, as the latter prevents unauthorized users from accessing the data while the former prevents authorized users from doing careless and malicious things.

- **ActiveSync device restriction.** Many employees have found their way on to corporate networks via ActiveSync without getting approval from IT. By restricting access to any device not being managed by the MDM tools, IT can ensure that it has visibility and control over all devices that access corporate information.
Mobile Application Management: Software Distribution, Lists, And App Stores

Mobile application management is beginning to dominate client conversations. Employee demand, consumer app stores, and in-house development are forcing the need for I&O professionals to have more granular control over application provisioning. Forrester recommends that I&O professionals prioritize the following mobile application management criteria (see Figure 3):

- **Remote software distribution and updates.** Many firms have customer applications that they develop in-house. The ability to distribute, maintain, and update these applications is a necessity for employee productivity and efficiency.
**Figure 3** The Mobile Application Management Criteria Of Mobile Device Management

<table>
<thead>
<tr>
<th>Vendors</th>
<th>Remote software distribution and updates</th>
<th>Whitelist/blacklist capabilities</th>
<th>App store restrictions</th>
<th>Enterprise-class app store</th>
</tr>
</thead>
<tbody>
<tr>
<td>AirWatch</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>FancyFon</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Fiberlink</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Good Technology</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Kaseya</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile Active Defense</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>MobileIron</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Motorola</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Notify Technology</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RIM</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sybase</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Symantec</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Tangoe</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trellia (acquired by Wyse Technology)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Virtela</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Wavelink</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Zenprise</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Source: Forrester Research, Inc.

**Whitelist and blacklist capabilities.** By setting a list of whitelisted applications, IT provides access to a specific list of approved applications on the device; blacklisting restricts access to unwanted or potentially harmful applications.

- **App store restrictions.** For varying workplace productivity and security reasons, some firms choose to restrict access to consumer applications stores as a whole, only allowing specific, IT-approved applications.
• **Enterprise-class app store.** As firms develop and procure applications for their mobile workforce, I&O professionals are increasingly identifying the need for an enterprise-class application store. Although still nascent technology, these stores allow users to access all the mobile tools they need to do their jobs while IT can manage and provision them all from the same console. As a part of an MDM solution, these tools also leverage policy engines, reporting, and access controls.

**Differentiating Criteria: Platform Support, Integration, And Availability**

Capabilities are emerging that differentiate solutions in this burgeoning market, such as location-based services and peripheral support. However, many Forrester clients continue to ask about platform support, integration with core IT service management, and expense management software when trying to select the right MDM solution. Forrester recommends that I&O professionals prioritize the following key differentiating criteria (see Figure 4):

• **Mobile platform support.** As previously mentioned, Forrester finds that I&O professionals will support multiple mobile platforms over the next 12 months: BlackBerry (84%), iOS (83%), Android (77%), and Windows Phone 7 (61%).

• **PC platform support.** As the line between the traditional desktop computer and mobile device continues to blur, vendors with client management backgrounds have expanded their solutions to offer MDM. These vendors are beginning to provide dashboards and reporting capabilities that include combined information from mobile devices and Windows-, Mac-, and Linux-based devices.

• **Service management integration.** As I&O professionals continue to industrialize their IT operations to deliver a consistent quality of IT service, a key MDM requirement in the future will be integration with core IT asset management and IT service management suites accessible to service desk employees.

• **Expense management.** Many firms look to telecom expense management (TEM) solutions to provide them with bill auditing and device life-cycle management. While most MDM solutions offer usage tracking, some have also partnered with TEM vendors to provide a full solution for their customers.

• **Global presence.** Mobile device management is still a maturing market comprising many smaller vendors. As a result, not all MDM solutions are available in all geographic regions. The majority of MDM solutions have roots in North America and are quickly expanding to EMEA and the Asia Pacific regions.
### Figure 4 The Platform Support, Integration, And Availability Criteria Of Mobile Device Management

<table>
<thead>
<tr>
<th>Vendors</th>
<th>Mobile platform support</th>
<th>PC platform support</th>
<th>Service management integration</th>
<th>Expense management</th>
<th>Global presence</th>
</tr>
</thead>
<tbody>
<tr>
<td>AirWatch</td>
<td>Android, BlackBerry, iOS, Symbian, Windows Mobile, Windows CE, Windows Mobile, Windows Phone 7</td>
<td>Selected Windows manufacturers</td>
<td>BES, APIs available for service management integration</td>
<td>Usage tracking, TEM via partners</td>
<td>Global coverage</td>
</tr>
<tr>
<td>FancyFon</td>
<td>Android, BlackBerry, iOS, Symbian, Windows Mobile, Windows Mobile</td>
<td></td>
<td>BES, Microsoft CA, SNMP systems</td>
<td>Usage tracking, TEM via partners</td>
<td>NA/EU (via indirect sales channel - carriers, solution partners, and systems integrators)</td>
</tr>
<tr>
<td>Fiberlink</td>
<td>Android, BlackBerry, iOS, Symbian, Windows Mobile, Windows Mobile, Win Phone 7</td>
<td>Windows, Mac, Linux</td>
<td>BES, APIs available for service management integration</td>
<td>Usage tracking, TEM via partners</td>
<td>Global coverage</td>
</tr>
<tr>
<td>Good Technology</td>
<td>Android, iOS, Windows Mobile, Symbian</td>
<td></td>
<td>Remedy, IBM Tivoli, and HP OpenView</td>
<td></td>
<td>Global coverage</td>
</tr>
<tr>
<td>Kaseya</td>
<td>Android, iOS</td>
<td>Windows, Mac, Linux</td>
<td></td>
<td></td>
<td>Global coverage</td>
</tr>
<tr>
<td>Mobile Active Defense</td>
<td>Android, iOS, Windows Mobile, Symbian</td>
<td></td>
<td>BES, Remedy, IBM Tivoli, HP OpenView, BMC Patrol</td>
<td></td>
<td>Global coverage</td>
</tr>
<tr>
<td>MobileIron</td>
<td>Android, BlackBerry, iOS, Windows Mobile, Win Phone 7, webOS, Symbian</td>
<td></td>
<td>BES</td>
<td>Usage tracking, TEM via partners</td>
<td>Global coverage</td>
</tr>
<tr>
<td>Motorola</td>
<td>Android, iOS, BlackBerry, Windows Mobile</td>
<td>Windows</td>
<td>APIs for service management integration</td>
<td>TEM via partners</td>
<td>Global coverage</td>
</tr>
</tbody>
</table>

Source: Forrester Research, Inc.
### Figure 4: The Platform Support, Integration, And Availability Criteria Of Mobile Device Management (Cont.)

<table>
<thead>
<tr>
<th>Vendors</th>
<th>Mobile platform support</th>
<th>PC platform support</th>
<th>Service management integration</th>
<th>Expense management</th>
<th>Global presence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notify Technology</td>
<td>Android, BlackBerry, iOS, Symbian, webOS, Windows Mobile, Windows Phone 7</td>
<td></td>
<td></td>
<td>Usage tracking, TEM via partners</td>
<td>Global coverage</td>
</tr>
<tr>
<td>RIM</td>
<td>BlackBerry</td>
<td></td>
<td></td>
<td></td>
<td>Global coverage</td>
</tr>
<tr>
<td>Sybase</td>
<td>Android, iOS, Symbian, Windows Mobile</td>
<td>Windows</td>
<td></td>
<td>Usage tracking, TEM via partners</td>
<td>Global coverage</td>
</tr>
<tr>
<td>Symantec</td>
<td>Android, BlackBerry, iOS, Symbian, Windows Mobile, Windows Phone 7, webOS</td>
<td>Windows, Mac, Linux</td>
<td></td>
<td></td>
<td>Global coverage</td>
</tr>
<tr>
<td>Tango</td>
<td>Android, iOS, BlackBerry</td>
<td>BES</td>
<td></td>
<td>Yes</td>
<td>NA/EU</td>
</tr>
<tr>
<td>Trellia (acquired by Wyse Technology)</td>
<td>Android, iOS</td>
<td>BES</td>
<td></td>
<td>Usage tracking, TEM via partners</td>
<td>Global coverage</td>
</tr>
<tr>
<td>Virtela</td>
<td>Android, BlackBerry, iOS, Symbian, Windows Phone 7, webOS</td>
<td>BES</td>
<td></td>
<td>Usage tracking, TEM via partners</td>
<td>Global coverage</td>
</tr>
<tr>
<td>Wavelink</td>
<td>Android, iOS, Symbian, Windows CE, Windows Mobile, Windows Phone 7</td>
<td>Windows, Mac, Linux</td>
<td>IBM Tivoli, HP OpenView, Unicenter, and any SMNP-capable management system</td>
<td>Usage tracking natively, additional functionality via Wavelink Telicost</td>
<td>Global coverage</td>
</tr>
<tr>
<td>Zenprise</td>
<td>Android, BlackBerry, iOS, Symbian, webOS, Windows Mobile, Windows Phone 7</td>
<td>BES, Remedy, IBM Tivoli, HP OpenView, BMC Patrol</td>
<td></td>
<td>Usage tracking, TEM via partners</td>
<td>Global coverage</td>
</tr>
</tbody>
</table>

Source: Forrester Research, Inc.
SEGMENTING THE MARKET: INNOVATORS, NEW ENTRANTS, BEST-OF-BREED, AND SERVICES

The MDM vendor landscape can be segmented into four distinct groups: innovators, new entrants, best-of-breed, and services. While the vendor landscape continues to proliferate, here are some worth short-listing:

- **Innovators: AirWatch and Fiberlink.** Although many vendors offer hosted infrastructure solutions, AirWatch supports flexible architectures in that it can be delivered through an on-premises solution, an appliance, or a SaaS solution. AirWatch's user-friendly, actionable management dashboard and competitive pricing have made it a top MDM contender for many firms. Fiberlink has offered a SaaS client management solution for years, and released its MDM solution in the second half of 2010. Despite being a relative newcomer to the MDM space, Fiberlink's single pane of glass, web-based console and experience with and commitment to security and compliance in the cloud computing arena has earned the vendor traction with the US federal government and a place on customers' shortlists.

- **New entrants: MobileIron and Zenprise.** Building off their strong on-premises and hosted infrastructure offerings, both MobileIron and Zenprise have recently released SaaS offerings. MobileIron has consistently appeared on client shortlists and RFPs for its on-premises solution and will look to deliver the same high-quality solution to firms seeking a cloud solution. Zenprise's on-premises and hosted offerings demonstrate the firm's commitment to network and application security, and those characteristics make its SaaS solution a strong choice for buyers looking for cloud-based deployment options.

- **Best-of-breed: Motorola Solutions, RIM.** Motorola's MSP solution can manage smartphones in addition to peripheral devices such as cash registers, scanners, RFID readers, printers, signature capture pads, and kiosks. Motorola Solutions also offers MSP as a managed service to customers who need help managing their population of large ruggedized devices and field service employee devices. RIM's BES is the gold standard for on-premises enterprise BlackBerry management. Last year, RIM introduced its BES Express cloud offering, which delivers more than 35 policies to get up and running quickly. RIM also acquired German MDM vendor ubitexx in May 2011 and announced plans to add support for Android and iOS to its on-premises MDM solution by the end of the year. However, it's not yet clear whether RIM will offer Android and iOS support as a cloud service.

- **Services: Good Technology, Mformation Technologies, and Sybase.** I&O should also explore managed mobility services if the time frame for deploying a behind-the-firewall solution is too long, too expensive, or if the infrastructure required is too complex. Most tier one mobile operators, such as AT&T, Bell Mobility, BT, Elisa, Rogers Communications, Sprint, T-Mobile, Telefónica, TeliaSonera, Telus, Verizon Wireless, and Vodafone, offer MDM as a managed...
service, and these solutions are often white labeled from Good Technology, Mformation, and Sybase among other vendors listed earlier. Global infrastructure outsourcers, such as Dell, Getronics (now part of KPN), HP, and IBM Global Business Services, are folding mobile services into their broader portfolio of managed infrastructure services.

• Specialists: Avema, Enterprise Mobile, and Virtela. Specialists like Avema and Enterprise Mobile offer managed mobility services, including MDM, and can even help customers select the solution most appropriate for their environment. Cloud service companies like Virtela offer a broad range of services for firms looking to deliver additional mobile solutions on top of MDM-like expense management.

WHAT IT MEANS

THE FUTURE WILL BRING MORE OF THE SAME — BUT FASTER

The smartphone and tablet markets have experienced — and will continue to experience — explosive growth as consumer spending picked up with the back-to-school season — and will continue with the upcoming holiday seasons. In corporate environments, smartphones have penetrated just 35% of workforces. As firms add support for employee-owned devices and move away from a one-size-fits-all model to support unique work requirements across user segments, MDM solutions are becoming must-have solutions for businesses worldwide. In the future, Forrester anticipates that:

• I&O managers will have their hands full with just BlackBerry, iOS, and Android support. The prevalence of multiplatform mobile strategies, coupled with support for employee-owned devices, has forced MDM vendors to focus on support that satisfies an extensive set of users. Expect vendors to focus specifically on differentiating their support for Android, BlackBerry, and iOS as well as to gauge enterprise interest in a possible fourth platform, specifically Windows Phone 7. Increased consumption of mobile applications is also pushing much of the development toward expanded application provisioning and security — because in large part of BYOD programs. Enterprise app stores will be the center of this innovation wave in 2012 and beyond.

• Vendor consolidation, strategic alliances, and white labeling will continue. The MDM landscape is ripe for further vendor consolidation, strategic alliances, and white labeling of solutions. Some recent notable examples include Nokia’s acquisition and eventual discontinuation of Intellisync, Motorola’s acquisition of Good Technology and its subsequent sale to Visto, HP’s acquisition of Bitfone, Tangoe’s acquisition of InterNoded, Good Technology’s acquisition of CloudSync, SAP’s acquisition of Sybase, McAfee’s acquisition of Trust Digital, and RIM’s acquisition of ubitexx — to name a few. Expect some smaller vendors to be prime acquisition targets by the incumbent vendors looking to round out their suites and by PC/client management vendors that view MDM as a natural extension to their strategies. Bottom line: Check back early and often on this space as acquisitions continue at a fevered pace.
True convergence of mobile device and PC management is inevitable but still years away. We’re still at least two to three years away from mainstream enterprise I&O managers being able to effectively manage all clients, including smartphones, desktops, laptops, tablets, ultrabooks, and netbooks, through a single pane of glass. Acquisitions and strategic partnerships and an eventual convergence of roles within I&O will drive more firms to explore the possibility. We remain years away from deep product convergence even though some MDM solutions technically support Win32 PCs and some PC/client management solutions support Windows Mobile and BlackBerry. It remains to be seen which vendors will take ownership of this convergence, but Forrester anticipates the PC/client management vendors to win out over the long term.

SUPPLEMENTAL MATERIAL

Companies Interviewed For This Document

AirWatch
Avema
FancyFon
Fiberlink
Good Technology
Kaseya
Mobile Active Defense
MobileIron
Motorola
Notify Technology
Research In Motion
Sybase
Symantec
Tangoe
Trellia (acquired by Wyse Technology)
Virtela
Wavelink
Zenprise

ENDNOTES

1 For 25 years, a one-size-fits-all approach to workforce technology worked just fine, but those days are fading fast. With overall adoption levels surprisingly low on the one hand, and yet with some employee groups racing ahead with Web 2.0 and other consumer technologies, it’s time for IT to give up on one-size-fits-all and instead master the real needs of employees. Workforce personas — we named them Michael, Diane, Oliver, and Andie — are a simple technique borrowed from consumer market research to help IT pros characterize and profile the needs of these different employee segments. Harness workforce personas to save money on the next rollout of Microsoft Office, anticipate adoption barriers for workforce technology, and increase satisfaction with advanced collaboration or mobility tools. The end game? Persona-driven provisioning. See the December 9, 2009, “Harness The Power Of Workforce Personas” report.

2 Groundswell technologies — social, mobile, video, and cloud — put tremendous power in the hands of customers. Only empowered employees can respond at the speed of empowered customers — and they’re often information workers outside of IT. We call these innovative information workers HEROes — highly
empowered and resourceful operatives. The HERO Index is a new tool we have developed to measure just how empowered and resourceful your own employees are. Our data reveals that some industries (like technology products and services) and job descriptions (like marketing and nonretail sales) harbor more HEROes than others. See the June 18, 2010, "The HERO Index: Finding Empowered Employees" report.

In 2016, Forrester projects that 63 million US information workers will telecommute at least part-time. Our recent survey of 4,985 US information workers indicates we're well on our way to hitting that mark. To cope with a more mobile and remote workforce, many organizations have bolstered deployments of laptop computers, smartphones, and collaboration software. But are these the technologies workers need to stay connected and productive? And are IT departments doing a good job delivering these tools? Forrester asked US information workers how important it was that IT provide these technologies and how well they believed IT delivered. See the August 17, 2011, "Does Your IT Department Support The Needs Of The Mobile Workforce?" report.

The commercial mobile device landscape continues to evolve dramatically, and the days are numbered for limiting IT support to a single mobile operating system (OS). Google Android and Apple iOS are joining RIM BlackBerry among the mobile OSes that IT must support, while Microsoft's release of Windows Phone adds yet another player into the fray — all of this signifying a profound shift in corporate IT road maps and new challenges in how infrastructure and operations (I&O) professionals must support them. See the August 3, 2011, "Updated 2011: The Mobile Operating System Wars Escalate" report.

I&O professionals worldwide are significantly altering their mobile computing strategies. Why? Because the prevalence of consumer smartphones, maturing enterprise-class mobile applications, the upcoming wave of slates and tablets that will be folded into the mix, and empowered workers are all driving I&O to change how it supports mobile devices. I&O professionals must meet the needs of workers while continuing to ensure that corporate data is properly managed and secured across all devices, regardless of who owns the hardware. Over the past six months, Forrester assisted 121 enterprise clients with developing or refining their mobile policy in an effort to meet these changing requirements. Forrester has identified 15 best practices that I&O professionals should use when crafting their new mobile policies. These practices keep corporate data secure, employees productive and happy, and costs down, while selectively embracing the consumerization of IT where appropriate. See the January 11, 2011, "Fifteen Mobile Policy Best Practices" report.

The years of limiting device choice to a single platform are over. Employee segments have drastically different technology requirements today. Users need to be provisioned with different application workloads, must have access to corporate resources while mobile and from remote locations, and prefer to select from multiple device types. As employees take advantage of consumer tools that meet their needs and applications become nearly ubiquitous, I&O professionals are hard-pressed to deliver the tools that employees need when they need them. I&O managers need to maintain varying levels of service and support and map them to their segmented workforce. Segments that require tablets will need access to different applications than those with PCs, while users with corporate-owned devices will need much greater levels of support than those employees who bring in their own devices. See the September 19, 2011, "10 Lessons Learned From Early Adopters Of Mobile Device Management Solutions" report.
8 Source: Forrsights Networks And Telecommunications Survey, Q1 2011.


12 Whether at home, on the road, or from an office, work is becoming something people do, not somewhere people go. In fact, 66% of information workers in North America and Europe already work remotely. Over time, this trend will have profound implications for everything from the location and design of offices, to IT’s provisioning of technology, to how business leaders marshal expertise. See the September 21, 2011, “The State Of Workforce Technology Adoption: US Benchmark 2011” report.

13 Understanding how information workers use smartphones and applications enables marketing executives across the mobile value chain to successfully develop products and services to address the needs of these workers. See the November 20, 2009, “Understanding Information Worker Smartphone Usage” report.
Forrester Research, Inc. (Nasdaq: FORR) is an independent research company that provides pragmatic and forward-thinking advice to global leaders in business and technology. Forrester works with professionals in 19 key roles at major companies providing proprietary research, customer insight, consulting, events, and peer-to-peer executive programs. For more than 28 years, Forrester has been making IT, marketing, and technology industry leaders successful every day. For more information, visit www.forrester.com.

Headquarters
Forrester Research, Inc.
60 Acorn Park Drive
Cambridge, MA 02140 USA
Tel: +1 617.613.6000
Fax: +1 617.613.5000
Email: forrester@forrester.com
Nasdaq symbol: FORR
www.forrester.com

Research and Sales Offices
Forrester has research centers and sales offices in more than 27 cities internationally, including Amsterdam, Netherlands; Beijing, China; Cambridge, Mass.; Dallas, Texas; Dubai, United Arab Emirates; Frankfurt, Germany; London, UK; New Delhi, India; San Francisco, Calif.; Sydney, Australia; Tel Aviv, Israel; and Toronto, Canada.

For the location of the Forrester office nearest you, please visit: www.forrester.com/locations.

For information on hard-copy or electronic reprints, please contact Client Support at +1 866.367.7378, +1 617.613.5730, or clientsupport@forrester.com.
We offer quantity discounts and special pricing for academic and nonprofit institutions.