Transitioning to a Mobile Workforce: Key Support Considerations for Enterprise Mobile Devices

An ENTERPRISE MANAGEMENT ASSOCIATES’ (EMA™) White Paper
Prepared for Bomgar
July 2012
Table of Contents

Executive Summary .......................................................................................................................... 1
The Mobile Revolution.................................................................................................................... 1
Ten Key Considerations for Enabling Workforce Mobility............................................................... 2
  #1 How will the organization establish control over devices that are employee owned? .......... 2
  #2 How will mobile support services be customized to meet unique end user requirements? ... 2
  #3 How will enterprise systems and data be secured to prevent inappropriate access? .......... 3
  #4 How will mobile devices be configured to support business services and to conform with business standards? .............................................................................................................. 3
  #5 How will mobile users gain access to critical applications that were designed for desktops? ... 3
  #6 How will business applications be delivered to mobile users? ............................................. 4
  #7 How will IT operations deal with the addition of new platforms to support? ...................... 4
  #8 How can incident management be performed on devices that are remote? ....................... 4
  #9 How will the mobile devices be protected from loss or theft? ............................................. 5
  #10 How will existing enterprise management resources be extended to also support mobile endpoints? ................................................................................................................................. 5
Adopting IT Support Resources that will Enable Workforce Mobility ............................................ 5
EMA Perspective .......................................................................................................................... 6
About Bomgar ............................................................................................................................... 7
Executive Summary

Enterprise reliance on mobile devices to drive workforce productivity and business profitability is not only increasing, it is accelerating. To remain competitive and achieve organizational goals, enterprises must adopt mobile solutions that extend business services to a mobile workforce and ensure their devices are reliable, effective, and secure. IT organizations, however, are challenged to add support for a number of new mobile platforms and meet emerging mobile requirements without substantially increasing operational costs and complexity. The successful transition to a mobile workforce requires the strategic implementation of new management processes and the introduction of integrated automated tools that extend current IT operational capabilities to mobile platforms.

The Mobile Revolution

We have entered the age of workforce mobility. No longer are business professionals tied to their physical office workspace in order to perform essential tasks. Thanks to advances in mobile technologies, employees are able to access a wide variety of business resources – including telephony, email, calendars, applications, and data – from almost any location at any time. This substantially accelerates workforce productivity and improves opportunities for collaboration with tools for video/online conferencing, screen sharing, and messaging. For employees, this also translates into greater flexibility to balance their work and private lives with telecommuting and the ability to operate out-of-home offices. Professionals that are required to provide out-of-hours support can certainly appreciate the convenience of never needing to leave their bedroom in order to respond to 3:00 AM emergencies. Further, organizations are able to employ the most appropriate personnel regardless of their physical geographic location, allowing for remote or branch offices to be located anywhere in the world.

The enterprise mobile revolution, however, is actually a fairly recent phenomenon. Although mobile devices – such as pagers, PDAs, smartphones, and tablets – have been around for quite some time, the past few years have seen a broad growth for enabling mobile capabilities across both horizontal (size of organizations) and vertical (type of organizations) business segments. What has fundamentally changed is the acknowledgement that enabling workforce mobility has become an essential practice for meeting organizational goals and achieving business success. A mobile workforce facilitates rapid customer response, improves business agility to respond to changing requirements, and increases employee accessibility to resolve business critical incidents.

It is ironic that many businesses which now rely on mobile capabilities never intentionally set out to transition to a mobile IT model. The “consumerization” of IT, which can trace its roots to the introduction of the iPhone in 2007, changed the way IT devices (and, in particular, mobile devices) were developed and marketed to focus on the needs of end users, rather than on enterprise requirements. Employees began purchasing these devices themselves for personal purposes, but extended their use to also assist in their job requirements. Recognizing and encouraging this trend, many organizations instituted “bring your own device” (BYOD) programs where they subsidized purchase of employee-owned devices either in part or in whole. Although this arrangement has proven extremely successful in improving workforce productivity and employee job satisfaction, it has resulted in a giant headache for IT managers. To begin, the number of platforms they are required to support has rapidly increased due...
Transitioning to a Mobile Workforce: Key Support Considerations for Enterprise Mobile Devices

To the little or no control they have over which devices are being purchased. In fact, many organizations have been taken completely off-guard by the sudden influx of new devices and operating environments (i.e., most popularly, iOS and Android) for which they are now obligated to manage and provide services. The problem is compounded by IT support organizations that lack the critical resources—such as budgets, staff, and management tools—to extend existing support services to mobile endpoints. Enterprises are often severely challenged to develop a clear plan for enabling workforce mobility that is comprehensive without increasing operational costs and complexity.

Ten Key Considerations for Enabling Workforce Mobility

Whether an organization is looking to adopt mobile technologies or already has a substantial mobile workforce that it now needs to support, a clear plan must be established that outlines how mobile devices will be supported. It is important that mobile management processes be proactive in nature (anticipating potential problems) rather than reactive (perpetual “firefighting”). Some support requirements will be obvious, such as the enabling of email access and the securing of any sensitive data that will be remotely accessed. Many requirements, however, are not so easily recognized, but also must be considered before implementing a management process. To help with planning for enabling mobile support, EMA has identified ten key questions that every organization should address in developing their mobile management plan:

#1 How will the organization establish control over devices that are employee owned?

Employees are, unsurprisingly, not so keen on allowing their employer to monitor or place restrictions on their personally owned devices. The more control an organization exerts over mobile device use, the more impact it will have on the employee’s personal use of the device. Making matters worse, end users will likely find ways of working around policies they find too limiting—such as by “rooting” or “jailbreaking” the device or by utilizing unapproved software and external services. To overcome this challenge, enterprises must strike a fine balance between establishing policies that are essential, but that are not unnecessarily limiting. Any restrictions or processes for accessing sensitive business data, applications, and services must be clearly defined and enforced. Put simply, if employees want to use their personal devices for accessing business resources, they must conform to the essential business practices. For example, before being given mobile access to the company’s intranet, employees may have to agree to allow IT to remotely wipe their device, including all personal information, should it be lost or stolen. The use of “sandboxing” and virtualization solutions that segment work resources from personal resources on mobile endpoints can also provide some relief, but it should be noted that users typically prefer not to have to continually switch between two completely separate environments on their device.

#2 How will mobile support services be customized to meet unique end user requirements?

Not all users are the same. Some business professionals will require broad access to business resources, while others will need little or none. Access to sensitive business applications, data and services should be restricted to only those personnel that actually require access in order to perform their job function. This means the availability of business resources must be delegated based on user roles or include some
other process for the authorization of their access. However, this process should be automated and tied into the organization’s enterprise identity management system (e.g., Active Directory), if possible, to minimize the impact on IT support. It is simply too time consuming to expect administrators to regularly patrol every individual mobile device to identify what requirements they have and how they are being used. Manual monitoring practices are also difficult to track and decrease accuracy due to the increased chance of human error.

#3 How will enterprise systems and data be secured to prevent inappropriate access?

Business data must be secured on enterprise servers, when in transit to remote devices, and on the mobile endpoint itself. Although mobile devices must be able to access business systems, that access must be restricted only to authorized users and only for access to resources for which authorization is granted. Any data that is downloaded to mobile devices must be encrypted to prevent inappropriate interception on LAN, WAN, internet, wireless, and cellular transmissions. Business data residing on mobile devices must also be protected from unauthorized duplication and rebroadcasting. In addition, mobile devices need to be protected from viruses and other malware and must be prevented from passing on any compromised software to other business systems. Administrator access to mobile devices must be secured as well. Encryption should be employed for data collection, remote device access, and the delivery of software updates. Finally, of course, passwords and security keys must be kept strictly confidential.

#4 How will mobile devices be configured to support business services and to conform with business standards?

EMA primary research has identified the configuration of email as the second-most critical mobile management capability today (just behind “data security”). This should be no surprise as email access was also identified as the single most important mobile function for business use and most end users lack the knowledge and information to connect with enterprise email systems without IT support. But email is just the beginning of configurations administrators need to perform. Many software elements – including applications, hypervisors, databases, and agents – may also require customization to operate in the business environment. Additionally, end users may require assistance with the configuration of the device itself and with establishing wireless access to the company LAN. All of this requires administrators to have a strong familiarity with the supported mobile platforms as well as the tools to configure them remotely so they can assist with enabling effective mobile configurations.

#5 How will mobile users gain access to critical applications that were designed for desktops?

Although many commercially available business productivity software vendors have or are in the process of porting their solutions to mobile platforms, propriety business applications must also be rebuilt to either run directly on mobile devices or over a Web interface that is mobile friendly. Developers must be sensitive to the fact that the smaller form factors (i.e., size and user interface) must be addressed and that there are a number of system limitations with mobile devices (such as CPU, GPU, memory, and storage limitations). There may also be difficulties meeting application requirements due to a lack of supporting services, such as Flash support. Despite all of these challenges, users will expect mobile application performance to be equivalent to what they are used to working with on desktop environments.
#6 How will business applications be delivered to mobile users?
Mobile users are familiar with the concept of downloading software from an “app store.” Business applications, however, are typically provisioned from Web portals and/or a variety of other distributions points. This can be very confusing and frustrating for end users that prefer to acquire their mobile software from a single source, and with some mobile platforms, going around the “app store” isn’t even an option. A consolidated mobile application distribution platform should be implemented, but it must also be able to deliver software for all supported mobile platforms. Additionally, end users will only want to be presented with applications applicable to their particular device. For instance, Android users will not want to have to sort through iOS applications, and vice versa. Further, enterprise mobile application distribution platforms need to limit access to authorized personnel for some software elements in order to meet security and licensing restrictions. All supported mobile business applications will also need to be continually updated with the latest editions and software patches.

#7 How will IT operations deal with the addition of new platforms to support?
IT support staff are currently not trained to support all mobile platforms (iOS, Android, BlackBerry, Windows, etc.). Typically, in fact, a support representative’s familiarity with mobile devices and platforms is limited to whatever device they happen to use themselves. This affects both their ability to support the devices as well as the mobile applications and services they will be delivering since they function differently on each mobile device type. Organizations will need to make strategic decisions on which mobile device platforms they are willing to support if they are going to limit services, but they must also be prepared to extend support to other platforms in order to meet expanding business requirements. (Let’s face it – as soon as a senior executive brings in his new tablet, that platform will need to be supported as well.) To ensure all IT staff members are able to support the influx of new mobile platforms requires a sharing of knowledge and a collaboration on management processes to ensure reps can leverage each other’s expertise and receive on-the-job training for supporting new platforms and devices. IT operations should also leverage support solutions that are platform-agnostic so reps don’t have to use a different set of tools for each type of device.

#8 How can incident management be performed on devices that are remote?
Help desk support requests for mobile devices are typically focused on usability and training issues. This is quite different from, say, desktop support, where the majority of support representatives’ time is spent resolving hardware and software failures. With mobile devices, end users are most often challenged with enabling access to and utilizing business applications and services. The chief challenge for IT support reps is working with remote users who have varying degrees of technical capabilities. Less technical users will need to be “talked through” every step of the problem evaluation, configuration, and remediation process. More knowledgeable users, on the other hand, can actually impede problem resolution by performing unnecessary or inappropriate tasks (i.e., “a little knowledge can be a dangerous thing”). In order to successfully guide remote users through a training or repair process, it’s extremely helpful if the reps can see what the user is seeing and/or view the system information as if they have the device in their hands. It is not practical or efficient for a rep to blindly talk a user through a repair process and hope they are following instructions correctly, particularly since the support rep may not be familiar with the mobile platform or application that is having the problem.
#9 How will the mobile devices be protected from loss or theft?
According to ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) survey-based research, one out of every nine mobile users will lose their device, and one out of every eleven will have their device stolen. If any of those devices contain sensitive business information or are authorized to have access to business resources, it could result in catastrophic financial and business loss. Organizations must have the ability to remotely track, lock, and/or wipe mobile devices that store or access business resources to inhibit any unauthorized use. To prevent these security measures from being circumvented, rooting and jailbreaking of the devices should also be prevented.

#10 How will existing enterprise management resources be extended to also support mobile endpoints?
Most enterprises have already invested heavily in operational support for IT investments and, in particular, for desktop systems. Rather than incurring the expense of duplicating the management resources, it is much more efficient and effective to extend existing services to also support mobile devices. This is particularly true with use of automated management tools. By utilizing a common interface for accessing all managed systems (i.e., servers, desktops, and mobile devices), administrative practices are simplified as support staff are able to use one familiar command set. Additionally, having a single location to record and review information about multiple supported endpoints will enable the correlation of incidents to perform root cause analysis and proactive problem prevention – as opposed to “swivel-chair management,” where administrators are challenged to review data on multiple interfaces. To minimize the financial and workload impacts of supporting workforce mobility, enterprises must adopt automated platforms that transcend endpoint platform types to provide a unified management experience.

Adopting IT Support Resources that will Enable Workforce Mobility
Enabling a mobile workforce can only be achieved with the adoption of automated management tools designed to support all mobile device platforms in the enterprise. Just as with desktops, these resources are invaluable for asset detection, provisioning, configuration and performance management of the endpoints. Incident and problem management processes are particularly enhanced and simplified with the use of management tools that perform information gathering and remediation tasks. To be effective, automated support tools must work hand-in-hand with remote access capabilities to enable prompt problem identification and remote management capabilities that will significantly reduce both Mean Time To problem Detection (MTTD) and Mean Time To problem Resolution (MTTR).

Recognizing the importance of unified endpoint management, Bomgar offers an appliance-based remote support solution that enables IT organizations to remotely access and support all endpoints in a support stack. Bomgar integrates directly with other service desk tools to provide a consolidated solution for supporting servers, desktops, laptops, kiosks, smartphones and tablets from a single, centralized console. The Bomgar solution supports granular role-based access, integrating with Active Directory or LDAP to automate configuration of user profiles, allowing them access to just those services required for the users to perform their job function. Mobile device platforms currently supported by Bomgar include iOS, Android, BlackBerry and Windows Mobile, and plans for support of Windows 8. Remote mobile support capabilities offered by the Bomgar solution include:
Transitioning to a Mobile Workforce: Key Support Considerations for Enterprise Mobile Devices

- **System data collection** – Detailed device and system status information is recorded for all supported mobile environments (iOS, Android, BlackBerry, Windows Mobile), providing valuable diagnostic details to aid in incident identification and resolution.

- **Secure end user chat** – Initiates immediate real-time chat sessions without requiring any additional software download beyond the remote support solution. Sessions can be used to converse with users, speeding time to resolution.

- **Encrypted file transfer** – All data transferred to and from supported mobile endpoints are secured with 256-AES SSL encryption, fully protecting data from threats and interception during transmission.

- **Remote control** – BlackBerry and Windows Mobile devices can be remotely accessed and controlled by Bomgar with full mouse and keyboard control in the same way reps can control desktop systems.

- **Screen sharing** – iOS and BlackBerry devices can capture and share screen shots so administrators can see exactly what errors or conditions end users are experiencing to more quickly diagnose a problem or provide guidance on device use.

- **Co-browsing** – For iOS support, administrators can view the same Web sites and Web apps that an end user is actively viewing on their device. In this way, administrators can more easily direct users in the use of Web based services or to help diagnose a related problem.

- **Configuration profile pushes** – Configuration profiles can be created and then pushed to supported iOS devices, helping to standardize the support stack to enable prompt problem resolution without the need for end user interaction.

- **Rep authentication and access** – Bomgar’s identity management processes integrate directly with existing authentication and security resources (such as LDAP, Active Directory, RADIUS and Kerberos) to ensure only authorized support personnel are able to remotely access mobile devices.

- **Session recording and audit** – Secure logging of remote session activities is also performed to ensure accountability. Bomgar keeps detailed logs of session activity, chat transcripts, transferred files and system information, plus video recordings of each session, and allows managers to track and log administrative activity, enabling multiple levels of managerial oversight.

**EMA Perspective**

As enterprise adoption of mobile devices continues to accelerate, requirements for supporting workforce mobility have been rapidly evolving. As recent as two years ago, primary enterprise concerns over mobile devices were limited to enabling email access and addressing security requirements. This has all changed. Now a full range of management requirements are attributed to mobile devices that are on par with industry standard practices commonly applied to desktops. Although currently there are distinct differences between support requirements for mobile devices and those for desktops (most notably around OS provisioning and application delivery), the two practices are most assuredly merging together. Advances in mobile technology are already blurring the lines between tablets and laptops, pointing the way to a near future that consolidates support of both environments into a single set of unified endpoint lifecycle management practices.
Transitioning to a Mobile Workforce: Key Support Considerations for Enterprise Mobile Devices

Organizations that have or are looking to adopt mobile platforms must lay the foundations now for integrated support that achieves the breadth of mobile requirements across all available platforms. These include ensuring endpoint performance, enabling user productivity, and meeting compliance objectives. Integrated management solutions, such as the remote management capabilities offered by Bomgar, achieve these requirements while minimizing impacts to the organization. By extending existing support infrastructures to mobile devices, administrator and support rep tasks are simplified without incurring substantial new operational costs. In this way, organizations can achieve mobile support capabilities that allow users the freedom to utilize mobile devices that will increase their productivity, empowering businesses with greater flexibility and responsiveness.

About Bomgar
Bomgar provides remote support solutions for easily and securely supporting computing systems and mobile devices. The company’s appliance-based products help organizations improve tech support efficiency and performance by enabling them to securely support nearly any device or system, anywhere in the world – including Windows, Mac, Linux, iOS, Android, BlackBerry and more. More than 6,500 organizations across 65 countries have deployed Bomgar to rapidly improve customer satisfaction while dramatically reducing costs. Bomgar is privately held with offices in Jackson, Atlanta, Washington D.C., Paris and London. You can find Bomgar on the Web at www.bomgar.com, or on Facebook, Twitter, LinkedIn and Google+.

About Enterprise Management Associates, Inc.
Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help its clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter or Facebook.

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. “EMA” and “Enterprise Management Associates” are trademarks of Enterprise Management Associates, Inc. in the United States and other countries. ©2012 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES™, and the mobius symbol are registered trademarks or common-law trademarks of Enterprise Management Associates, Inc.