
J. Gold Associates

•

www.jgoldassociates.com

Managing Mobility in the Enterprise

A J. Gold Associates White Paper

July 2005

Contents

Managing Mobility in the Enterprise	1
<i>Introduction.....</i>	<i>1</i>
<i>Major General Mobility Trends.....</i>	<i>1</i>
<i>Diversification of Mobility.....</i>	<i>3</i>
<i>Where can mobility deliver ROI for the business?.....</i>	<i>3</i>
<i>The need for management of mobile workers/devices.....</i>	<i>4</i>
<i>Mobile management: what's in a name?.....</i>	<i>5</i>
<i>Is it necessary to have a mobile-aware management solution?.....</i>	<i>6</i>
<i>What should companies look for?.....</i>	<i>7</i>
<i>Is mobile management separate from security?.....</i>	<i>8</i>
<i>When to Deploy Mobile Management.....</i>	<i>9</i>
Conclusions	10
<i>About the Author</i>	<i>10</i>
Appendix: Case Studies.....	11
<i>Hurley Corporation</i>	<i>11</i>
<i>City of Oakland Police Department.....</i>	<i>12</i>
<i>University of Georgia New Media Institute.....</i>	<i>13</i>

Managing Mobility in the Enterprise

Introduction

Most enterprises currently view mobility as a relatively minor portion of their overall IT budgets, despite its being consistently placed within the top 5 initiatives of the next 3 years in surveys of business executives. As a result, with few exceptions, companies have failed to adequately plan for and manage the growth of mobility over the past few years, and more importantly, have failed to plan for the accelerated growth which will occur over the next few years. Mobile empowerment enables employees to take back office systems to the point of interaction with the customer, no matter where their customer might be. As a result, customers receive a higher level of service and exhibit a higher level of satisfaction and loyalty to their supplier. Employees achieve higher productivity and greater job satisfaction. Mobility, therefore, is a key competitive differentiator and business imperative. But managing mobility is different and requires new tools and processes.

While local area network (LAN) connected notebook computers and off-site workers are currently handled by a standardized IT process architected for an inside-the-company-facilities model, the massive growth of mobility over the next 3-5 years will leave company IT organizations unable to cope with the new mobile reality unless they rethink the existing strategy. One of the greatest challenges to both business and IT groups within companies over the next 5 years will be effective deployment and management of mobility in the workforce, over a wide array of devices, connections and applications. This paper will highlight some of the areas mobility will expand, and address how companies should advantageously manage such mobility. Failure to effectively tackle the mobility challenge will leave companies with inefficient operations and at a major competitive disadvantage through poor customer service, higher cost of operations, and lack of flexibility. Mobility, therefore, must be included in any enterprise strategy.

Major General Mobility Trends

The enterprise is being overtaken by a race to mobility. Users are demanding anytime, anywhere computing capability, and anytime, anywhere access to corporate applications as well. Most companies are having great difficulty keeping up with the insatiable demands of end users. Indeed, we expect over 50% of users at enterprises to be outfitted with notebook computers within the next 3 years (increasing from approximately 35% currently), and well over 95% of these devices will be wirelessly enabled. Further, we expect that knowledge workers will be mobile 50%+ of the time within the next 2-3 years, working from a diverse location mix of office, home, travel sites, customer sites, etc. Finally, personal mobile devices such as handhelds and smart phones, most of them wirelessly enabled, are being deployed as data access devices. The majority of mobile workers (65+%) will be enabled with such capabilities within 3-4 years, adding diversity to corporate application deployments and forcing companies to deal with a wide array of client devices.

Managing Mobility in the Enterprise

However, not all mobile deployments are driven by end users. Forward thinking enterprises are also adopting mobility to drive more effective and efficient operations, particularly in field force operations (e.g., field service, delivery, logistics, field sales, health care delivery). Task-specific devices and applications are extending business critical systems (e.g., ERP, CRM, SFA) to automate previously manual field operations (e.g., order entry, trouble ticketing, dispatching), through deployment of data-enabled mobile devices, including ruggedized notebooks, handhelds and smart phones. This class of user generally views the mobile device as an on-the-job tool, rather than a general purpose computing device, and is likely to have access only to this one device which is a mission critical component of the person's daily duties.

The lines of inside-the-company IT boundaries will blur significantly as smart phones (e.g., BlackBerry, Treo, Nokia Communicator, Symbian, Windows Mobile devices) increasingly become common. Their use will be popularized through email access, but they will rapidly be enabled with access to back office systems (e.g., ERP, CRM, SFA), as users demand more functionality and companies understand the benefits of extended mobility. We expect 75% of enterprise users to move to smart phone devices from their current "dumb" phones by 2008, requiring organizations to offer increased connectivity options to those users, as well as support and device/application management. Further, wireless broadband connections (e.g., public WiFi, faster cellular networks, WiMax) will supplement existing broadband (DSL, cable modem) and will increasingly enable end users to stay connected at almost any location (e.g., hotel, airport, home office, customer site), thus further driving adoption of mobile technologies. However, wireless connections will never be as fast or as reliable as wired connections. Companies deploying mobile wireless solutions must include a strategy to deal with the variations in connection types, reliability, and specific mobile management challenges that wireless connectivity poses.

Scalability will become a key requirement of any successful mobile initiative. With a growing number of users, connections, devices and applications, scalable infrastructure will require the ability to add and manage users without requiring a fundamental re-architecting of the support systems each time a new user group or application is deployed. For this reason, companies must choose infrastructure that can easily be expanded to include all device types, user types and usage models (e.g., wired, wireless). Mobile management must embrace and enable this fundamental need for scalability.

Few enterprises currently have adequate plans to adapt to this changing environment by deploying sufficient infrastructure and application support. Even fewer (well under 10%) have sufficient plans to manage and secure such diversity of devices, connections and location. This is a scenario which is deemed totally unacceptable to the fixed desktop/server environments of most companies where management tools exist (e.g., Microsoft Systems Management Server (SMS), CA Unicenter, Tivoli, etc.), although their relatively high level of complexity often limits their usefulness within organizations. One of the key challenges of the next 5+ years for enterprises will be maintaining control of

Managing Mobility in the Enterprise

their mobile work forces. Managing Mobility will become a competitive edge to those companies who do it right, and a substantial Achilles Heel to those who don't.

Diversification of Mobility

In many organizations, the mobile application environment has been seen as a notebook computing-centered phenomenon. Users obtain notebooks, take them on the road with them, work with them from home over increasingly common broadband connections, and utilize them at many remote sites. While this model has increased productivity in many organizations, the notebook has been treated as essentially a portable desktop (e.g., same operating system (OS), same application build, same help desk staff, same IT tools), even though it is often used in very different circumstances/environments. However, we are in the early stages of a major transition from company environments where mobility was equated with notebooks, to one where a diverse mix of devices is present (e.g., Palm and Microsoft Pocket PC handhelds, BlackBerry email devices, Nokia and Palm smart phones). We expect this diversification of device types to continue unabated. In fact, we expect that within the next 2-3 years, many users will have 2-3 data access devices which are used on a regular basis and which must be supported by enterprises.

We do not expect notebooks to exit the scene. Rather, we expect specialized devices to be deployed for specific tasks (e.g., ruggedized handhelds for industrial workers, smart phone devices for wireless email, wireless handhelds for sales force, etc.). Organizations will attempt to standardize on specific families of devices to limit device diversity, but this will not be possible for all groups across the entire enterprise with varying needs. This means that IT groups will not only be forced to continue to manage notebooks, but will also be increasingly forced to include other data-centric pervasive devices in the mix. The days of WinTel domination and the standardization it brought are over when it comes to the mobile world. This will fundamentally challenge the tools, processes and policies put in place to deploy, secure and manage applications.

Where can mobility deliver ROI for the business?

With all these difficult challenges, why would companies consider expanding their mobile deployments? Mobility offers some very significant return on investment (ROI) to companies that do it well. Route drivers carrying handhelds show an increase in sales and an ability to make more stops in a day via efficient routing. Warehouse workers with scanner-equipped devices eliminate the double entry keying of previously paper-oriented systems, allowing for greater accuracy and accelerated billing. Sales people in the field can close sales faster by using a wireless device to check on inventory levels and tell customers when products will be delivered. All of these instances of mobile-equipped users provide ROI benefits to organizations. And they are just a few examples of an ever expanding array of companies using mobility to enhance their businesses through increased sales, better asset management, improved inventory turns, etc. Companies ultimately able to scale to encompass all field workers across all lines of business will exhibit major bottom line advantages.

Managing Mobility in the Enterprise

The need for management of mobile workers/devices

Few companies do an effective job at managing their mobile workforces. In fact, few companies understand the optimum management techniques for mobile workers. They either ignore the problem, or see mobile management as an extension of existing desktop management operations. This is a fundamental mistake, as managing mobile devices has unique characteristics that are unlike fixed desktop management.

The first step in an effective mobile management strategy is to set usage policies, which need to be communicated to, and agreed upon by the end users. Lack of this critical first step is the biggest impediment to successful completion of mobile projects. Once set, these policies can be enforced with mobile management tools. Policies that need to be considered for a variety of mobile devices (especially smaller personal devices like handhelds and smart phones) include:

- making sure password protection is set to “on” (fewer than 5% of users set password protection on unless they are required to do so by company mandated enforcement),
- determining what files can be downloaded/synchronized and by which users,
- limiting personal files on the device (e.g., music, video, games, etc.),
- setting up encryption when needed (to protect sensitive corporate data from loss, especially for loss prone devices),
- enforcing connection/VPN standards that ensure maximum protection for company data transmission
- updating personal fire walling/antivirus and application,
- enabling device lock down, and “device kill” functions (e.g., if the device doesn’t connect with the company network/server within a fixed amount of time it is presumed lost and is therefore wiped clean, or at the least specific critical files are destroyed).

The next step in defining a mobile management strategy is to determine which applications are to be made available to the mobile user and on which devices. Typical applications include email, sales force automation, field service applications, dispatching, extended CRM, etc. All of these applications can offer payback to the organization if deployed and managed effectively. Yet few companies who roll out mobile worker applications add management capabilities at the outset. While some application providers offer some limited amount of management capability, this is usually limited to their specific implementation/application, and should not be considered as a broad-based mobile management tool.

Finally, a company must set a mobile security policy that is complimentary to existing company security policy, but is inclusive of some of the unique characteristics of the mobile environment (e.g., often disconnected from the network, higher loss rate of equipment, potential addition of personal files, etc.). While several mobile security suites exist (e.g., Credant, Pointsec), they generally lack any significant management capabilities

Managing Mobility in the Enterprise

beyond their own security needs. It is, however, becoming common for mobile management vendors (e.g., Afaria from iAnywhere, Intellisync, iPass) to increasingly include security functionality as part of their overall management suite, some through partnership with security vendors and some through their own tools.

Policies that lead to effective mobile device management can offer a significant payback in several ways. Well managed mobile deployments result in greater end user satisfaction, fewer support calls, more timely application deployment/updates, and fewer devices returned to the IT department. All of this can add up to some real savings. Organizations that deploy effective mobile management solutions have 10%-15%+ lower overall Total Cost of Ownership (TCO) than companies that deploy mobile devices/solutions without a mobile management plan. While TCO varies by device type and application, it is not uncommon to see \$150-\$250 savings per user per year. With mobile management tools costing \$50-\$100 per user (depending on functionality and volume), it is clear that mobile management has an attractive ROI.

What is equally as important to realize are the consequences of not having an adequate mobile management strategy. Companies failing to deploy adequate mobile management tools face non-productive users who must often struggle with old or outdated applications, out of date files on their devices, and the need to send devices back to the office for updates. Indeed, many mobile workers are thus forced to become their own IT support staff, preventing them from focusing on their own jobs, or worse, causing them to abandon the application altogether as too hard to use and nonproductive. This is a very costly approach to mobile management, and can add a 20%-25% burden to the generally already stretched thin support and help desk staff as they walk end users through the problem resolution process.

Mobile management: what's in a name?

Mobile management suites are fundamentally different than standard desktop management suites. Desktop management suites generally are architected for always connected, fast network, behind-the-firewall interaction. Further, they are generally available only for Windows OS based systems. While some suites have built limited extensions for mobile workers (e.g., SMS), they still fundamentally assume a connected approach. These suites fail to provide the functionality needed by the mobile user.

Mobile suites are inherently architected differently to work within the constraints of the mobile environment. They assume that most mobile users are only occasionally connected, that the speed of those connections can vary over some great range (from dial up to broadband), and that the connections are prone to be disconnected at any random time. Further, these suites assume that they cannot schedule an update at a specific time (say, 2 a.m. when many LAN based suites push updates to end user devices), since the devices randomly connect to the company network. Even wireless devices that profess to full time connectivity go into and out of coverage.

Managing Mobility in the Enterprise

Mobile management suites must be architected to manage a wide range of diverse devices, from fully capable notebook computers running Windows, to a variety of handhelds (Palm, PocketPC and potentially Linux), to smart phone devices from a wide array of vendors with unique aspects beyond simply diverse operating systems (e.g., Symbian, Windows Mobile, PalmOS, RIM, Linux, etc.). Finally mobile suites must be very efficient with bandwidth and provide for interrupted connections without unforeseen negative consequences for the device. That means they must include store and forward capability to download for later use, have bandwidth throttling for efficient delivery, check point restart capability, high levels of download compression, failsafe recovery so only complete updates are installed, and an intelligent agent running on the mobile device to make all of this happen transparently to the end user of the device. Creating an intelligent agent optimized for various platforms is no trivial task, and is something not available from general desktop management suites.

Mobile management suites generally have to connect to a more diverse range of applications as well. Since most fixed applications can tap into SMS or some other standard management suite, they do not have to provide extensive integrated management functionality. However, in a mobile scenario, such integration must be redirected to the mobile management suite to enable applications to take advantage of their functionality. This requires that mobile management suites provide an API that can be integrated with the enterprise application. Such integration is crucial if organizations are to take maximum advantage of mobile suites.

Mobile management is used for everything from small file updates to full remote provisioning of devices in the field. As such, they must have complete and easy-to-use management consoles that allow a policy-based (by user, group, department, etc.) definition of services. Most suites are now offering a connection to directory services (e.g., LDAP, Active Directory) to make this task somewhat easier. Further, most suites now include a connection to management consoles used within many organizations (e.g., Microsoft Mobile Management Console (MMC), Tivoli, Unicenter, etc.) so as to provide a more integrated approach to overall end user management.

Is it necessary to have a mobile-aware management solution?

With the preponderance of mobile enterprise users looming on the immediate horizon, companies must be proactive in defining strategies to deal with the mobility factor. Most companies have management strategies and tools in place to manage infrastructure systems (e.g., servers, networking, storage), and some have deployed desktop management tools. But of the companies that have deployed desktop management (less than 25% of enterprises), few have plans to take these to mobile users beyond the notebook, and even notebooks are generally managed only when connected directly to the company network. But even if they have such mobility management plans, few of the current tools can serve the needs of the enterprise without having the mobile advantage inherent in a purpose-built management suite for mobile. What makes the DNA of mobile management tools different?

Managing Mobility in the Enterprise

These suites must be able to communicate with a variety of devices over a variety of networks at a variety of speeds. Moreover, they must focus on reliability of data delivery, while at the same time limiting the amount of data delivered (through file data differencing, data compression, etc.). These optimizations allow them to take maximum advantage of the limited bandwidth, and to counteract any problems caused by intermittent connections and non-specific user connection times. They must have a variety of clients built for a great variety of devices (and getting greater over time) that must all work with the common back end infrastructure of the mobile management suite. And finally, they must be capable of providing a single point of integration for the widest array of file and data types (e.g., OS patches, antivirus updates, DB syncing, application deployments, device attribute management, etc.). We do not expect the major vendors (e.g., Tivoli, CA, HP, Microsoft) to catch up to the specifically mobile capabilities of the mobile management suite vendors for at least 3-5 years. Companies can't wait that long to implement mobile management. Nor will end users wait to have manageable mobile systems that don't require heavy user intervention and the resultant frustration that it causes (and the help desk support burden it creates).

What should companies look for?

In choosing a mobile management suite, enterprises should be aware of some key points to evaluate. What are some of the selection criteria for these packages?

- *Policy-based management* – can users be defined as individuals, groups, communities, and have specific management capabilities applied to them? Can this be easily changed, and can this be tied to a directory?
- *Little or no user involvement* – mobile management (indeed all end user management) should be completely transparent to the end user. Things should happen in background and should, as much as possible, cause little to no performance degradation or screen indications. Users should also be unable to disable the management system.
- *Broad functionality requirements* – can the suite function with a wide variety of applications and data requirements? Does it have the needed interfaces to allow customization and additions?
- *Directory integration* – can the suite interface with already defined directory structure and policies so as not to require a stand-alone or duplicate directory?
- *Scalability* – can it provide management for a large number of users with a large number of devices? Though most companies start small, it is likely that ultimately, many users will have multiple devices and eventually substantially increase the number of devices in the enterprise, even beyond the actual number of users.
- *Single console for all network/application/device/security requirements* – can the tool provide a single console from which it can define, control, deploy and maintain all aspects of the device, application, network and security?

Managing Mobility in the Enterprise

- *Web-based console* – can the tool be managed from a web based console from any standard browser, allowing management from local or remote locations, and on a variety of devices?
- *Support for diversity in devices, platforms, and networks* – does the application support a variety of devices, connections and platforms, and will the vendor continue to expand on the device types and OS flavors?
- *Security components* – does the application provide at least a minimum set of security capabilities within the product? Can it be integrated with higher level security tools?
- *Bandwidth aware* – can the tool adjust for whatever bandwidth is available for the particular connection (e.g., not delivering massive file updates on a slow connection)?
- *Dashboard* – can the tool provide a management dashboard of information on processes, users, devices, performance, etc.?
- *Backend management integration* – can the tool integrate effectively with other back-end management infrastructure already deployed within the organization without needing to retrain existing staff already familiar with the application?

The above criteria should be used to evaluate any potential management application to be deployed within the enterprise infrastructure. Only then can a company be assured it is maximizing its capability to effectively and efficiently manage mobile users and devices.

Is mobile management separate from security?

Security management suites share some of the same characteristics as general device management suites. They must be able to query the device and see what is installed. They must be able to search out and replace files. They must look at the various device settings that affect the overall level of security. And they must have a policy-driven console that allows a company to execute security settings based on individuals, groups, job function, etc. There is a logical affinity to the types of functionality in both security-oriented and general device management-oriented applications.

So, can one tool be deployed for both purposes? Generally, for adequate levels of security, the answer is yes. Mobile management solutions that intersect security and management, with a high level capability for policy management and a unified management interface are attractive to many organizations that don't require the extreme levels of security necessary in some specialized instances.

Specialized high levels of security require uniquely formatted code and the capability of working deep within the internals of the device (e.g., FIPS security and encryption, antivirus, firewalls) and are more adequately provided by targeted security suites. However, most security suites do not cover many of the more general management functions inherent in the management suites (e.g., asset management), and so need to be supplemented with management suites in any event.

Managing Mobility in the Enterprise

We expect an increasing level of basic security to be integrated into general management suites (e.g., patch management, personal firewall configuration, AV updates), with most management suites optionally offering a product from a security partner for security enhancements (e.g., AV, encryption, firewall). Indeed, many management suites have already developed such partnerships, but this is a fluid marketplace and many more non-exclusive partnerships will arise as security needs change over time and OS vendors add their own inherent capabilities. Since management suites are generally easier to deploy, operate, and integrate into existing management environments, we expect most companies to start with the management suites and their included security features, and then add high level security components as the need arises. In fact, we would not be surprised to ultimately see some mobile management vendors acquire security vendors and incorporate the complete solution into their applications.

When to Deploy Mobile Management

Currently, the majority of companies using mobile device management suites have deployed this technology after the fact (i.e., several months to years after deploying the mobile technology). We believe this is a mistake. Companies should plan to deploy management as an important component of any mobile application. Indeed, companies who do not will face increased costs, more difficult support challenges and more difficult upgrades (e.g., device provisioning, change management, system refreshes). Although many application vendors offer some basic level of mobile management, it is generally tied to their own applications and does not offer the greater breadth and diversity necessary to support a wide variety of devices and applications that will most certainly be deployed within the organization over time. Although mobile management suites add a cost to mobile deployments, it is generally a small fraction of the overall expense (less than 5%), but can save a significant amount (10%-15%) in ongoing TCO.

Indeed, there are inherent risks of not deploying mobile management. Examples exist of companies deploying applications to the field that have a wrong version of the code or a corrupted database of customers, products, prices, etc. End users who are not aware of this may commit the company to a bad business deal through such an error, or may not be able to service the customer in a timely manner, potentially losing a sale. Mobile management tools that allow on-the-fly change management/corrections would have replaced the bad file and/or information automatically, preventing such an occurrence. In this case, mobile management can provide a margin of error in business operations, and prevent either a bad decision, or a disgruntled customer, and offer real bottom line payback.

Conclusions

Mobile management must be a key component of any enterprise mobile strategy if it is to succeed. Failure to include adequate levels of mobile management will substantially increase TCO, prevent the most efficient deployment and degrade the end user experience. Mobile management is different than desktop management and specific tools must be deployed to make it work properly. A tool that provides the most flexibility to include a growing set of device types and connection types will be the most productive tool for the organization in the long term, as the mobile market will continue to shift for at least the next 3-5 years. Companies who have mobile applications already deployed and who do not currently have a mobile management suite should act quickly to implement such technology, or risk being overwhelmed with high cost of ownership and increased support burdens. Finally, security and management go hand in hand, and a coordinated approach to mobile security and mobile management should be implemented as soon as possible. No matter how good the mobile technology deployed at a company may be, mobile management can be the difference between a solution succeeding and failing.

About the Author

Jack E. Gold is Founder and Principal Analyst at J.Gold Associates. Mr. Gold has over 35 years in the computer and electronics industries, including work in imaging, multimedia, technical computing, consumer electronics, software development and manufacturing systems. He is a leading authority on mobile, wireless and pervasive computing, advising clients on business analysis, strategic planning, architecture, product evaluation/selection and enterprise application strategies. Before founding J. Gold Associates, he spent 12 years with META Group as a Vice President in Technology Research Services. He also held positions in technical and marketing management at Digital Equipment Corp. and Xerox. Mr. Gold has a BS in Electrical Engineering from Rochester Institute of Technology and an MBA from Clark University.

Appendix: Case Studies

Hurley Corporation

Hurley is a leading provider of facility cleaning and ancillary services. The company contracts almost exclusively with large-scale property managers, including many airports and shopping malls throughout Canada and the United States. The company views their effective management of people and the implementation of leading edge technology at the front lines of their business, as crucial to their continued leadership in the industry; their resident managers as well as their entire fleet of cleaners carry handheld devices, which allow them to be more efficient and productive. Hurley placed barcodes in areas of their customers' buildings where they clean, such as restrooms. Each time a Hurley worker cleans an area, he scans that barcode with a Symbol PalmOS device. The scan creates a time-stamp and a location stamp. The handhelds are synchronized with an onsite computer that generates detailed reports given to the customer identifying which areas were cleaned and when.

Using Afaria, Hurley automatically pushes weekly updates to the control application, as well as software and company information to their devices. Hurley was able to wash their hands of the old costly and labor-intensive method for more than 150 employees located in over 80 sites. Together Afaria and Canadian reseller Kilobytes Computers Inc., streamlined the process of managing mobile devices in the field while ensuring accurate information exchange, integrity and security of Hurley's network and the devices connected to it. With Afaria in place, Hurley can be very proactive in pushing things like virus signature updates down to the mobile devices. What's more, Afaria provides additional security features like password authentication, to protect the company's data. These security features, including the ability to automatically and correctly install anti-virus updates, translate into real monetary savings for the company. Without Afaria, Hurley would have a lot more downtime with remote computers. If the computers were to get a virus, and there were any OS vulnerabilities on the machines, that virus could wreak total havoc on the network, causing a tremendous amount of very costly downtime.

"With Afaria in place, our ROI has been significant," states Anthony Talarico, IT Director at Hurley. "We've reduced the monthly number of helpdesk calls by 83% and the duration of the remaining calls by 60%. We also enjoy a 93% reduction in the time IT staff spend updating software. We reduced travel costs by 80% and eliminated all costs associated with shipping devices. The overwhelming initial success of implementing Afaria, made our CIO look like a hero."

City of Oakland Police Department

The Oakland Police Department employs approximately twelve hundred people, including seven hundred police officers on their front lines. Approximately 400,000 people reside in the community they serve which encompasses fifty-three square miles. The department now employs high-tech methods for fighting crime by providing patrol cars and motorcycles with computers that link up to vital policing information. However, the vehicles can only receive information while within range of their 802.11b wireless network. If a car leaves the network area before a download is complete it loses valuable information. The Oakland Police Department needed a solution that would easily provide officers with the most up-to-date information.

Afaria, from iAnywhere, now enables the department to send large files including wanted posters, missing persons information and crime statistics to the vehicles and to update those files automatically. There are 802.11b access points at main transportation points throughout the city. When a vehicle comes within coverage, a small script triggers the Afaria client, contacts the server and the files are updated. During the thirty to sixty seconds that it takes to update, Afaria checks to see that the computer has the latest version of all software packages used on that system. If an upgraded version or maintenance patch is available, it's automatically sent to the computer and installed. If an officer must leave the coverage area before a download is complete, the point of interruption is marked and the remaining data is delivered seamlessly when the officer returns to any of the areas served by the wireless network. Remote-troubleshooting capabilities allow headquarters to see what's going on with the onboard computers, enabling them to prevent problems before they start, replace corrupted files and more. Department IT administrators can manage the software on any of the over 200 laptops from a web browser or server without assistance, allowing the police officers to focus on fighting crime.

“Before we deployed Afaria, the department updated its officers on dangerous situations via paper flyers called Officer Safety Bulletins”, stated officer Inez Ramirez.

“Unfortunately, the photocopied images were often of poor quality. Also, if the officers misplaced the flyer, or if there weren't enough copies for each officer, they were without crucial information. Lack of information could translate into dangerous situations and prevent the police from solving crimes. By allowing headquarters to provide officers with up-to-date information, Afaria is truly helping us drive crime prevention and law enforcement.”

Managing Mobility in the Enterprise

University of Georgia New Media Institute

The New Media Institute (NMI) at the University of Georgia is chartered to discover and demonstrate new, innovative ways that mobile technology can have a positive impact on business and quality of life. The NMI was seeking a way to reduce the management burden of maintaining software and settings on mobile devices. In this unique environment, devices are constantly being handed out to different people, have many applications and tools installed on them, and the network environment continually changes.

NMI selected HP iPAQ Pocket PCs as its delivery platform for various mobility projects and procured one hundred of these devices. To showcase downtown Athens, GA and support local retailers, NMI created an Athens portal called The Cloud, which provides users with an easy, one-stop way to access information about local events, special opportunities and promotions. Naturally, NMI wanted to demonstrate these projects to a wide audience including business leaders, government officials, other academic institutions etc. As it set about doing so, it discovered it had a problem. "Managing the Pocket PCs turned out to be a nightmare," explains Scott Shamp, Director of NMI. "We found that even though we lent these devices out to people on a daily basis, they treated them as if they were their own. So they felt quite comfortable changing settings and installing new software. Additionally, after they returned the devices the batteries would often run down and crucial settings were lost. Managing these devices so they were always ready to operate as originally configured proved to be a formidable challenge. We also needed a way to update the software on the devices without dragging them all back to our office, stacking them next to an active synch console and reloading them that way."

NMI found the remedy to its management nightmare in Afaria, from iAnywhere. NMI deployed the Afaria client on all of its Pocket PCs and began using it to deploy and support its mobile applications. "Using Afaria ensures that the software and settings are always in order so we can demo our applications at any time," Shamp explains.

"Our focus at the New Media Institute is on applications and content. We don't want to have to devote a lot of time to manage the infrastructure and devices. Thanks to Afaria, we can focus on understanding how mobile media can be used to enrich people's lives and stimulate economic development and growth. It's freed up our human capital and given us the confidence to tackle bigger projects and more projects because we know we don't have to deal with the mundane aspects of managing the delivery mechanisms."