IBM Software
Thought Leadership White Paper

January 2012

Getting a better grip on mobile devices

Solutions and strategies for managing both employee-owned and enterprise-owned equipment

IBM

Contents

Introduction

The increasing use of smartphones and tablet computers as business tools has brought organizations and their employees new levels of productivity, flexibility and mobility. But their use is a double-edged sword, bringing with it new levels of complexity to IT management and security.

To cope, organizations need to put into place new policies for business use. Will employees be permitted to use their personal devices, or is there a company-owned standard? What is the most effective management technology, for the environment? What management tools—full suite or point solutions—will meet IT needs for manageability and availability, as well as business needs for cost-effectiveness?

And organizations always need to ensure that devices and data remain secure in an environment where loss and theft are common.

On today's fast-moving, highly competitive smarter planet, where data gathering, information sharing and decision making must continue regardless of the user's location, the mobile device

is destined to continue growing in popularity and importance. And as smartphones and tablet computers expand their roles from personal communications devices to key interfaces for enterprise applications, the accompanying opportunities for business growth and the challenges for IT management will demand the same exacting standards that organizations apply to the rest of their technology environments.

The consumerization of IT is changing device management

Smartphones, tablet computers and other mobile devices are in the enterprise to stay. One recent survey of smartphone users found that 83 percent of users considered their device more important than their morning cup of coffee. Some 79 percent said they use their smartphone more than their office or home phone to conduct business. And 34 percent use it more than their computer.[1]

The use in business of a device that began in consumer electronics—sometimes called the "consumerization of IT"—can significantly empower employees. Allowing employees to use their personal devices for work, as many users prefer in order to avoid carrying multiple devices, lets them select the platform and form factor with which they are most comfortable. It enables them to move seamlessly, anytime anywhere, from personal to business functions. Allowing employees to use their own devices can also save organizations the cost of equipment purchase.

Security is a key driver of mobile device management

Even when used only for email and calendar access, a smartphone can contain confidential and sometimes regulated business information. An unsecured device stolen from a briefcase at a meeting or left behind in a taxi can easily put sensitive information into the wrong hands.

Worse still, if the device can access even more sensitive business applications, any device theft or loss, employee termination, hacking or corruption can mean the loss of unique information created with those applications. And it may give the thief, finder, former employee, hacker or malware purveyor access into the organization's data stores or centrally managed business applications.

Security, as a result, is a paramount reason for managing smartphones, tablet computers and other mobile devices. Effective mobile device management enables IT to deploy, configure, command and control endpoint security technologies on a wide range of devices. It enables integration and management of best-of-breed mobile security technologies with an enterprise management solution.

Similarly, effective management controls enforce security policies, such as a requirement to enter a personal identification number (PIN) before the device can be activated. To guard against data theft, IT should be able to remotely wipe the device clean of company-related contents.

Managing mobile applications is the next big thing

For mobile devices, voice and email were just the beginning. These were followed by the ability to easily download consumer applications directly from the device. The next step is the development and deployment of business applications through enterprise application stores. This will make mobile versions of third-party software for functions such as customer relationship management or software developed for the organization's unique business or technology needs widely and easily available to authorized users. An effective mobile device management solution will provide IT with the tools to deploy and manage these applications, and it will integrate with other solutions and services designed to create and support applications.

Mobile device management solutions can also support compliance with regulatory requirements by ensuring that device configuration or security solutions are properly deployed and managed. Management solutions can help enhance device performance and employee productivity by managing settings such as screen resolution. They also can track and assess software use to ensure that the organization has the proper number of licenses—neither too many nor too few—for its employees' devices.

IT organizations need mobile device management solutions that can be integrated with existing management infrastructure—enabling smartphones and tablet computers to be treated as part of the overall IT environment and eliminating the need for independent solutions for mobile device management. An effective solution is scalable to support the rapidly growing number of devices, cross-platform to manage the diversity of devices, and secure to support device and data integrity in out-of-office environments. Vendor services can include development of business applications, an enterprise application store for easy distribution of applications to devices, and outsourcing to relieve the infrastructure requirements and IT workloads as it speeds and streamlines device management.

Solutions for mobility: Application lifecycle management

While some aspects of the development of a mobile application are unique, the application development lifecycle follows the same pattern as for other kinds of software. Application lifecycle management (ALM) is necessary to ensure controlled development and delivery of high quality mobile applications within the budget constraints and time objectives. Even more important is that lifecycle management functions be integrated with each other and also with the tools needed for uniquely mobile development tasks. IBM Rational® software offers industry-leading solutions for lifecycle management that are augmented with mobile-specific capabilities for design, coding, security analysis and testing. By leveraging the publicly available Jazz technology for tool integration and collaborative team development, Rational addresses the full mobile development project lifecycle with traceability from inception to completion.

The management application: Suite vs. point solutions

From the user's perspective, employing a mobile device—especially an employee-owned device—to support business applications and communications can simplify work processes. One major enterprise has reported an average time savings of 47 minutes a day, about 10 percent of the typical workday, and increased productivity when employees were allowed to use the devices with which they are most familiar and comfortable.[2]

From the IT perspective, however, the proliferation of mobile devices and the accompanying diversity of operating platforms—most commonly those running Apple iOS and Google Android operating systems—creates complexity in management. The downside of simplifying users' processes with complex and diverse backend technologies can create heavy IT workloads, management headaches and increased chance of error. Problems can be compounded when IT attempts to manage diverse mobile devices using point solutions that address only specific management tasks, platforms or devices.

And while existing device management solutions may be effective at handing traditional endpoints, they typically are not well adapted for the special requirements of mobile devices. The lack of solutions for managing both traditional and mobile endpoints, as a result, has forced IT organizations to use standalone solutions for managing mobile devices. Yet as the number and functionality of devices grows, the need for an integrated suite solution becomes increasingly important.

A unified approach with centralized management efficiencies, enhanced visibility into diverse devices and their configurations, and consistent cross-platform reporting can play a key role in getting under control what can be a mammoth task, if handled piecemeal.

Significantly, a unified approach enhances security and streamlines reporting for mobile devices. Unified control manages diverse devices in a consistent manner, eliminating gaps that can occur with multiple point solutions in the way security is applied and the way vulnerabilities are reported. The result can simplify operations for the user and support greater security for the organization.

Solutions for mobility: IBM Global Technology Services

IBM Mobile Enterprise Services offers solutions designed to address enterprise mobility challenges across the entire mobile device lifecycle—from procurement and deployment to mobile device management and security to custom application development and deployment. Flexible solutions that accommodate a variety of mobile devices address a wide range of worker requirements, from day-to-day device management and support to application upgrades and coordination of deployments, rapid on-boarding of new users, support and problem resolution for end users and assistance with device configuration, setup and troubleshooting.

Management technology: Agents vs. agentless control

Any organization that allows employees to use their personal mobile devices for work sooner or later encounters the same question: What technology should IT use to manage a device that belongs to an individual? The debate continues regarding agent-based versus agentless management, as there are advantages and disadvantages to each.

Agent-based management places a small piece of "agent" software on the device itself that interacts with server-based management software to enable functions such as turning the device on or off, changing configurations, managing applications, enforcing encryption or wiping data and applications from memory. Advantages lie in the significant levels of control and extensive capabilities that this approach enables. Remote management, controlled by IT as needed, can be automated to ensure all operations are carried out and that they function correctly. The disadvantage lies in the requirement to install the agent on the mobile device: Users may not want the organization to place management software on their personal smartphone or tablet.

Agentless management employs a synchronization approach that requires users to connect to a central management site to initiate management functions through the corporate email system. The advantage lies in the fact that no software from the organization resides on the device, making this approach more palatable to many users. Disadvantages lie in the reduced control over devices: IT has fewer capabilities at its disposal and cannot enforce continuous compliance.

A third management technology approach, however, does exist. Balancing different IT organizations' needs for control and security with the users' preference for a less intrusive approach, the most effective mobile device management solutions enable both agent-based and agentless capabilities. This approach also can reach a larger number of operating platforms than a single approach—a significant advantage where some operating systems do not allow agents to be installed on devices and where management capabilities also vary with the OS.

Solutions for mobility: IBM Cognos software

IBM Cognos® Mobile enables users to interact with trusted business intelligence content on tablet computers, enabling them to seamlessly view and interact with business reports, dashboards and analysis either offline or online. Supporting timely and accurate decisions based on up-to-date information, the solution makes it easy to get to the right level of information when users need it, including location-aware intelligence that provides information based on the user's location. The ability to leverage existing business intelligence content and a single administrative environment helps IT keep up with the demands of users on varied devices.

An emerging focus on the enterprise app store

Capabilities for mobile device management are rapidly evolving—but IT preferences are already beginning to emerge that favor suite solutions, combine agent-based and agentless management, and deliver high scalability, reliable security and cross-platform functionality that integrates with the organization's other IT management solutions to create a unified management approach.

Security management, inventory management, policy management and software distribution will be core functions, with capabilities such as Software as a Service (SaaS), managed and outsourced services, custom software development and support for app stores growing in significance.

The enterprise application store, in fact, is central to the evolution of smartphones, tablet computers and other mobile devices from basic communications to highly functional business capabilities. The success of the evolution, however, will require a number of supporting functions—from policies that reinforce business operations and support users, to reporting that delivers insights for better and expanded functions, to security measures that reduce risk. Specific functions available now and anticipated in the coming years include:

- Security management to guard against unauthorized use or corruption of data due to theft, loss, hacking, malware attacks or employees moving to the competition
- Provisioning applications directly from the app store to the mobile device
- Monitoring of software use and device configurations to ensure compliance with industry and government regulations
- Policy creation and management that integrates mobile devices with the technology infrastructure and supports business goals

To ensure application performance and compliance, management solutions will automate solutions such as application updating and monitoring, configuration monitoring and remediation, and role-based user access.

Solutions for mobility: Managing network expansion

Smartphones and tablets are driving increased data volumes—requiring, as a result, new strategies from IT administrators. Often, these strategies involve network expansion, traffic distribution or network optimization. In the case of network expansion, IBM Tivoli® Netcool® tools, with the highly scalable tiered architecture of Netcool/OMNIbus, can help manage the alarms and events from the larger networks. Netcool tools can help collect the network statistics and provide reports and information for capacity planning.

IBM solutions deliver a new management paradigm

IBM Endpoint Manager for Mobile Devices, built on BigFix® technology, enables organizations to provide security and manage smartphones, tablet computers and other devices based on the Apple iOS, Google Android, Nokia Symbian and Microsoft Windows Phone platforms.

Leveraging the IBM Endpoint Manager infrastructure, which provides a single platform for managing servers, desktops, laptops and mobile devices running Windows, UNIX, Linux and Mac operating systems, this solution provides a unified approach for managing diverse devices. Consolidating management across the infrastructure, IBM Endpoint Manager for Mobile Devices:

- Delivers a flexible and powerful paradigm for managing employee- and corporate-owned mobile devices using a combination of email-based and agent-based management, while preserving the native device experience
- Ensures security functions by configuring and enforcing passcode policies and encryption—and selectively wiping enterprise data when devices are lost, stolen or compromised
- Automatically identifying non-compliant devices and denying email access or issuing user notifications until corrective actions are implemented

IBM Endpoint Manager for Mobile Devices provides real-time visibility into the state of mobile devices and gives administrators advanced functionality for managing those devices. As a comprehensive "single source of truth" for managing up to 250,000 devices from a single management server, IBM Endpoint Manager for Mobile Devices can shorten update cycles, improve the success rates for provisioning, reduce IT and help-desk labor requirements and boost end user productivity.

Solutions for mobility: IBM Maximo software

The IBM Maximo® Mobile Suite provides remote access to Maximo Asset Management processes, giving IT administrators the ability to use mobile devices to support compliance, improve efficiencies, increase productivity and enhance decision making. The Maximo solution delivers the ability to conduct asset audits, maintain asset configurations, and receive, track and maintain inventory. IT administrators can exchange data with the application server using real-time wireless, dial-up or docking cradle connections. And they can store and forward data when continuous connections are not feasible.

Supporting enterprise application stores to serve mobile devices, IBM Endpoint Manager for Mobile Devices provides policy-based installation, closed-loop verification and the ability to manage software distribution from a single, unified point of control. It delivers high first-pass success rates with minimal impact on network performance. And it offers user self-provisioning of authorized applications and software packages.

Application management capabilities automatically track installed applications, offer recommended applications and detect blacklisted applications. For managing devices, IBM Endpoint Manager for Mobile Devices captures and stores detailed device data, including inventory data such as device model and serial number, usage data such as last connection time, and hardware information such as firmware and memory, as well as operating system version, location information and network details.

Support features enable management and troubleshooting of devices that can streamline IT functions and reduce the workload on the organization's help desk. Remote diagnostics capabilities put real-time device data at administrators' fingertips with capabilities to assist end users in resolving IT issues, helping ensure that device configurations remain current and compliant with organizational policies.

Solutions for mobility: IBM Lotus applications

Employees today expect to take their desktops with them on their mobile device, stay engaged with professional networks through collaboration tools and access web content wherever they work. Customers also expect access to web content from mobile devices. Security-rich IBM mobile software and services can provide productivity and social collaboration tools on mobile devices. IBM Lotus Notes® applications, email, instant messaging, exceptional web experiences, professional networks, business intelligence reports and online meetings all are supported on a wide variety of smartphones and tablets.

Solutions for mobility: Application development and deployment

IBM is developing a set of capabilities for software developers who are building visually rich, interactive mobile applications that will work across a variety of mobile devices. These capabilities provide a set of application services, enterprise connectors, application and device management features, and accompanying integrated tooling—all implemented using industry-standard web technologies to maximize existing investments in skills and infrastructure. In addition, the capabilities can help development organizations to control who has access to specific applications and updates, get insight into application use and add security measures to ensure that application data and access is safe and secure. The full spectrum of mobile development approaches including native, hybrid and web will be supported.

Adopting an action plan paves the way for success

With the business use of smartphones, tablet computers and other mobile devices continuing to grow rapidly, it is not too early for organizations to plan to actively manage these mobile resources. A number of steps are necessary for implementing an effective mobile device management strategy.

Steps to mobile management success		
Inventory devices	Locate and identify the devices currently in use in the business environment, including the numbers of employee- and corporate-owned devices. Project the numbers expected to be in use 24 months from now and which applications they will be accessing	✓
Identify features	Determine which features the organization requires in a mobile device management solution	✓
Evaluate solutions	Outside a lab environment, test and evaluate potential solutions, checking scalability to meet the organization's growing needs, time to implementation and ease of operation	✓
Develop policies	Create or update relevant policies and training for device and application use and for role-based application and data access	✓
Consider costs	In selecting and implementing a solution, take into account the full range of costs, from software licensing to factors that influence the total cost of ownership including hardware purchase and maintenance, system implementation and related consulting fees, staff training, system administration and upgrade costs	✓

Conclusion

As the business use of smartphones, tablet computers and other mobile devices increases, organizations are facing device and application management needs that do not fit the traditional endpoint management paradigm. To meet these needs, organizations are putting into place new policies, determining the most effective management technologies for their respective environments and selecting management products for their unique needs.

In the face of the complexity that huge numbers of devices and multiple operating systems bring, however, the traditional reliance on point solutions that manage mobile device management separately from the rest of the IT infrastructure is proving to be inadequate. The need to speed and streamline management, avoid ballooning IT workloads, integrate mobile device management with management of the full IT infrastructure, and more efficiently serve users is driving adoption of a more comprehensive and unified management approach.

IBM Endpoint Manager for Mobile Devices gives organizations an effective and efficient way to manage the growing number of mobile devices—owned by employees as well as the organization—used in business today. Eliminating the need to implement a separate infrastructure solely for mobile devices, this unified solution provides high levels of application and security management across diverse mobile devices, including those utilizing the Apple iOS, Google Android, Nokia Symbian and Microsoft Windows Phone operating systems.

Leveraging IBM's leading ability to manage complex technologies and business environments, IBM Endpoint Manager for Mobile Devices provides comprehensive coverage from mobile device management to application development, support for app store development, outsourcing and security management.

For more information

To learn more about IBM Endpoint Manager for Mobile Devices, contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/tivoli/solutions/endpoint/mdmbeta

About Tivoli software from IBM

Tivoli software from IBM helps organizations efficiently and effectively manage IT resources, tasks and processes to meet ever-shifting business requirements and deliver flexible and responsive IT service management, while helping to reduce cost. The Tivoli portfolio spans software for security, compliance, storage, performance, availability, configuration, operations and IT lifecycle management, and is backed by world-class IBM services, support and research. For more information on Tivoli software from IBM, visit: **ibm.com**/tivoli

Additionally, IBM Global Financing can help you acquire the IT solutions that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize an IT financing solution to suit your business goals, enable effective cash management, and improve your total cost of ownership. IBM Global Financing is your smartest choice to fund critical IT investments and propel your business forward. For more information, visit: **ibm.com**/financing

IBM Corporation Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
January 2012

Please Recycle

IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion. Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision. The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

[1] Bradley, Tony, "Business Professionals Choose Smartphones Over Coffee," *PC World*, April 13, 2010, http://www.pcworld.com/businesscenter/article/194137/business_professionals_choose_smartphones_over_coffee.html

[2] Miller, Robert E. and Varga, Joe, "Benefits of Enabling Personal Handheld Devices in the Enterprise," Intel Corporation white paper, May 2011, http://www.intel.com/content/dam/doc/best-practices/inte-it-it-leadership-benefits-of-enabling-personal-handheld-devices-in-the-enterprise-practices.pdf

TIW14127-USEN-00