Consumerization of IT Brings New Mobile Computing Challenges

Kaseya Mobile Device Management extends robust IT and security policies to all systems, ensuring availability and security of business data out in the field.
Today’s user is always on the go, working from the road, customer sites, a sidewalk cafe or home office. Powerful new mobile devices from smart phones to tablets enable this agility, giving employees the information and tools they need where ever they need to work. However, as business data migrates from servers, desktops and laptops to remote devices, these systems need to be brought under the organization’s existing IT systems management strategy. For business continuity, security and compliance reasons, organizations need to extend the same robust IT and security policies to mobile devices.

This white paper will discuss:

- The unique requirements of mobile computing in today’s business environment
- The problems of existing mobile device management solutions
- The characteristics of an ideal solution
- How Kaseya solves these mobile device management issues and concerns

Consumerization of IT Hits the Mobile Market

Given the agility of today’s users, mobile computing is more than just laptops and home computers. Constantly-on-the-go employees access business data, email and applications from a variety of mobile devices from smart phones to tablets—even eReaders. Instead of souped-up phones these devices are viewed by users and by management as computers—no less important to an organization’s mobile computing strategy than laptops, desktops or servers.

According to a survey compiled by the 451 Group, 71.2 percent of businesses now allow personal devices to be used for work. By encouraging the use of personal devices, organizations are able to allow users to get the device they want—as opposed to a three-year-old Blackberry—without having to foot the bill. The problem, however, is that this mobile computing strategy greatly exposes business data to loss or theft while still building in a price per device for monitoring, maintenance and support.

The problem may lie with the devices themselves. Anthony Juliano, a senior partner with Landmark Ventures, a strategic and financial advisory firm for Fortune 500 companies, suggests that unlike the personal computer which was first conceived as a business tool, mobile devices today are designed for consumers first and businesses second. This shift in thinking has led many engineers to value usability and design over security, manageability, integration and other features that businesses require, posing a serious challenge for the corporate IT organization that has to manage these devices.

Organizations of all stripes and sizes are finding it difficult to standardize mobile device management and ensure the devices’ performance, availability and security. Juliano’s Fortune 500 clients are no different, finding that they do not have the policies and procedures in place in order to deal with managing employees’ personal devices. Specifically, organizations are having problems dealing with basic maintenance, security, business continuity, data usage and billing.

Basic Maintenance

Guess who users call when they are unable to access business email on their personal devices. It isn’t AT&T or Apple. It’s their organization’s IT department—despite the device not being under the purview of the IT organization. Businesses are finding it increasingly necessary to dedicate help desk resources to ensure the availability of users’ personal devices even though the systems were not procured by the organization.
Security and Business Continuity
What if a device is stolen or lost? A mechanism needs to be in place that either recovers the missing device or wipes it clean. As business information continues to decentralize into the field, organizations need to expand their ability to protect their data.

Data Usage and Billing
Users accessing business information, email and applications on personal mobile devices are going to see their data usage spike, inching their monthly service bill higher and higher. Do organizations have to reimburse users? What constitutes personal use versus business use? Is there a way to differentiate? Should organizations even try?

Problems with Existing Solutions
Existing mobile device management solutions include powerful functionality intended to solve these issues, but many fall short in many regards. While device auditing capabilities are robust, most solutions don’t truly understand what devices are being used by users and where they are. Just as important, the solutions often don’t know what data is being accessed and how secure it is on distributed mobile devices.

These shortcomings lead to a decentralized and inconsistent mobile device management strategy. Today’s disparate devices require organizations to purchase, deploy and maintain disparate management tools, one each for every mobile platform in use by employees—whether it’s iOS, Windows Mobile or Android. In addition to being a management and administrative headache, this makes it tough to reliably push out applications, update them and issue a patch. With so many mobile platforms in the market—and a lack of a central management tool that can manage across those platforms—organizations are finding it difficult to implement standard policies and to properly allocate expertise and resources.

Most importantly, the typical mobile device management solution does not integrate with existing IT systems management frameworks that may already be in place to monitor, update and maintain traditional IT infrastructures made up of desktops, laptops and servers. Instead, they serve as yet another management tool that requires capital expenditure, operational investment, training and support.

The Ideal Solution Should be Integrated
A complete solution needs to integrate mobile device management into the organization’s existing IT systems management strategy, creating a truly holistic solution that applies the organization’s IT and security policies to every machine that accesses business information—regardless of platform, operating system or physical location.

You’ve already developed, tested and implemented a robust IT systems management strategy that covers your traditional infrastructure. Why wouldn’t you simply extend it to all devices?

This expansion allows you to enforce an employee use policy that ensures personal mobile devices that access business information fall under the management purview of the IT organization, enhancing your organization’s existing business continuity, security and compliance programs. It also lays the groundwork for differentiating business use from personal use— and everything involved with that.

Keys to an Ideal Mobile Device Management Solution:
- Ensure complete coverage of all mobile devices and know where they are deployed
- Achieve visibility into all devices (OS, apps, minutes, data consumption, etc.)
- Be able to remotely deploy data and applications on devices and enforce settings
- Secure business data, including the ability to remotely lock and wipe phones
- Protect business data, including the ability to back up data, files and apps
The Kaseya Mobile Device Management Module

Recognizing that all systems and devices that access business data need to be managed robustly, securely and completely, the Kaseya Mobile Device Management Module is integrated directly into the Kaseya IT Automation Framework, effectively extending existing robust IT policies and procedures to all devices that log onto the corporate network to access business data and applications. The central Kaseya dashboard gives IT organizations the visibility they need to efficiently, consistently and reliability track, update and back up mobile devices.

Because of the unique architecture of cellular networks and proprietary hardware platforms, administrators can push out the Kaseya agent to mobile devices through text messages or a Web link. Once installed, the administrator has complete visibility into the device, including serial number, operating system, firmware status, installed applications and other inventory data. Administrators can then push out mobile applications, operating system upgrades and security patches, ensuring the device is running optimally and securely. Lost or stolen devices can also be locked and wiped remotely.

Unlike traditional mobile device management solutions, the Kaseya agent is largely autonomous, able to complete executions when the device isn’t logged onto a network, ensuring remote control even when the network is down or when the device has logged off. These executions can be triggered manually by an administrator or set to run automatically when certain thresholds or triggers are met. The agent-based architecture saves network bandwidth and data usage, alleviating some the billing concerns of users.

Automation inherent in the Kaseya framework and the solution’s unique agent-based architec- ture make the module ideally suited to manage mobile devices. It is integrated with the Kaseya IT Automation Framework, provides visibility and control into mobile devices and automates much of the manual administration associated with mobile computing, providing cost-effective IT systems management across the organization—even for systems not procured by the business.

Benefits of Kaseya Mobile Device Management:

- Extend IT systems management polices to mobile devices, including the iPhone, Android, BlackBerry and Windows platforms
- Protect business data no matter where it sits or where it is accessed
- Reduce help desk requests for mobile devices through remote and automatic management capabilities
- Manage all devices from desktops and servers to mobile devices from a single pane of glass for consistency and transparency throughout the organization

Kaseya is Integrated

According to Juliano from Landmark Ventures, today’s dynamic business environment requires his clients’ IT staff to be cross-trained in multiple mobile platforms. It only makes sense that organizations deploy a management tool that is similarly cross-trained, so basic maintenance can start to be automated—just as traditional IT systems management has been automated.

 Fortunately, mobile device management is consolidated through Kaseya’s Web-based dashboard, giving administrators visibility and control into thousands of devices at once, including servers, desktops, laptops, smart phones and tablets. Disparate management policies such as patch, security, monitoring and email are centralized in one location while administrators have the tools to take action to enforce compliance of multiple types of machines.
Kaseya Provides Visibility and Control

Kaseya allows administrators to view mobile devices out in the field—regardless of their location. Knowing their exact location and status is the first step in enforcing IT and security policies and allows you to provide access to email and mobile applications to users on the move. Kaseya also gives administrators the ability to track lost or stolen devices in real time with the help of GPS and other location tracking technologies.

However, all the visibility in the world is useless without the ability to make changes on tracked devices. Kaseya gives administrators the ability to remotely power up and down lost or stolen devices, set off an alarm so the user can find it or—in extreme cases—wipe the device and lock it down. Administrators can also remotely back up devices, push out applications, adjust settings and protect the device from malicious malware.

Combining control with visibility through the Kaseya IT Automation Framework helps organizations ensure all their mobile devices are in compliance with internal IT and security policies as well as government regulations like Sarbanes-Oxley and HIPAA.

Kaseya Mobile Device Management Allows You to:

- Automate email configuration and settings on mobile devices
- Collect detailed inventory information in a central repository that can be easily accessed by administrators and technicians for fast resolution
- Remotely install and uninstall mobile applications
- Track location of mobile devices in real time
- Back up and restore contact lists
- Lock, wipe and reset lost or stolen devices

Kaseya Enables Cost-Optimization through Self-Service and Automation

With hundreds of different devices from dozens of platforms, mobile device management can be expensive. Disparate tools require capital investment, on-going maintenance and training. Consolidating management through one solution—one that is already managing your systems infrastructure—can save you a lot of headaches and budget.

Kaseya is a cost-effective way to track, maintain, update, secure and protect smart phones and tablets at the same service levels as your other systems. Through automation and a proactive management strategy, Kaseya helps organizations lower their administrative pain while improving uptime, enhancing security and increasing user productivity.

Kaseya frees up your administrators’ time by automating many of the repetitive tasks that plague most IT organizations. Imagine automating the configuration of mobile devices for users visiting a remote office. Why not have the smart phone automatically join the corporate wireless network when a user walks into a remote office for the first time? Automation is inherent in the Kaseya IT Automation Framework, helping IT organizations eliminate many of the manual, labor-intensive, repetitive tasks that plague IT systems management. Kaseya also empowers users to conduct much of the basic maintenance on their own through Kaseya’s self-service portal. Users can download pre-approved mobile applications, update their operating system and reset their password without help desk resources.

Empowering user self-service and easing the administrative hassles associated with basic maintenance allows organizations to reallocate IT resources and expertise to other, more strategic projects. Instead of configuring email on an iPad, your technician can be developing a new mobile CRM application that helps streamline the sales cycle. Ideally, your IT focus will then shift from reacting to issues to proactively preventing problems from occurring in the first place, leading to a much more efficient and less costly IT management strategy.
Conclusion

The consumerization of IT is forcing organizations of all sizes to address growing mobile device management concerns. An ideal solution should be integrated with the organization’s existing IT systems management apparatus, effectively extending existing robust IT and security policies in place for traditional infrastructures to mobile devices. Kaseya Mobile Device Management gives organizations the visibility and control they need into their mobile devices while ensuring they are in compliance with the organization’s policies. This integrated and automated approach standardizes IT systems management across the organization and all systems in a cost-efficient, optimized manner.

Contact Kaseya Today

Contact Kaseya today for more information and to request a live demo of our powerful IT Systems Management solution.

About Kaseya

Kaseya is the leading global provider of IT Systems Management software. Kaseya solutions empower virtually everyone — from individual consumers to large corporations and IT service providers — to proactively monitor, manage and control IT assets remotely, easily and efficiently from one integrated Web-based platform.

Go to www.kaseya.com/download for a FREE trial.

Visit: www.kaseya.com  |  Email: sales@kaseya.com  |  Like: Facebook.com/KaseyaFan  |  Follow: @KaseyaCorp

©2011 Kaseya. All rights reserved. Kaseya and the Kaseya logo are among the trademarks or registered trademarks owned by or licensed to Kaseya International Limited. All other marks are the property of their respective owners.