Successful law firms deploy the right MDM tool to effectively gain control of data in motion.

Executive Summary

In short order, mobile computing has rocketed to the forefront of business computing, with network traffic and law firm data shifting from stationary desktops to in-motion devices seemingly overnight. In fact, some now consider mobile apps and devices to be the lifeblood of law firms.

According to the latest International Legal Technology Association (ILTA) survey, more than 50 percent of respondents cited mobility themes as the trends most affecting legal IT professionals. The reason: Firms want to give lawyers the tools they need to do their jobs more effectively and productively.

Like any sea change, the mobility revolution brings a host of new data security and device management challenges. IT shops struggle to deploy consistent controls across an array of varying software and device types.

Mobile device management (MDM) tools help solve these issues by allowing IT administrators to gain cross-platform control of devices. The strategy is to optimize the functionality and security of a mobile communication network while minimizing cost and downtime.
The Situation

It’s no secret that consumerization is changing the technology landscape at law firms. Fully 94 percent of lawyers use smartphones, and 88 percent of firms say they support tablet use, according to the ILTA 2012 annual survey of nearly 500 law offices.

The same survey also revealed a continuing embrace of the bring-your-own-device trend: More than 40 percent of legal firms permit BYOD.

In addition, voice-to-text mobile applications are beginning to gain traction. For example, use of Nuance Communication’s Dragon Dictation mobile version is up 4 percent from a year ago, the survey says.

Although the productivity gains from mobility can drive billable hours, having data in motion represents a paradigm shift at law firms. Previously accustomed to building security fortresses around data and systems, firms must now deal with 21st Century business realities.

The widespread proliferation of mobile devices puts unprecedented computing power and information at the fingertips of individuals throughout the organization. Today, legal data moves around on smartphones in the pockets of employees or travels on tablets to homes, clients and courthouses.

As legal IT staffs struggle to deploy controls across disparate apps and devices, MDM solutions can fill the void. Robust and mature MDM tools provide advanced capabilities to address a legal firm’s unique operating environment and keep costs in check while simultaneously ensuring that staff stays productive.

MDM — The Basics

The introduction of personal mobile devices into an enterprise network creates a number of security concerns that were less relevant in the days of centrally owned, managed and configured computers. Mobile device management solutions give administrators the ability to reassert control over the mobile devices attached to their networks, regardless of operating system (OS), hardware type or ownership status.

Key Features to Consider

Today’s MDM solutions offer a variety of features to meet the needs of legal firms:

- **Security management**: Because the salient reason to adopt MDM is security, related capabilities are the top priority for selecting the best fit for a given firm. MDM often includes the ability to remote wipe, enforce passwords and encrypt data.

- **Asset management**: Today’s MDM solutions permit the remote completion of all critical device management tasks, such as taking an inventory of enrolled devices. The same holds true for applications, which MDM solutions can detect, monitor and change. Other functionality includes pushing out apps to enrolled devices and gathering statistics on user adoption of external or internal apps.

- **Cross-platform capability**: According to ILTA, more than 70 percent of law firms currently support multiple mobile device platforms, making multi-OS support a necessity.

  Many modern MDM solutions support Apple iOS, Android, Symbian and Windows OSs. And because many lawyers continue to use BlackBerry devices, most firms will need an MDM solution that works with BlackBerry Enterprise Server as well.

- **Configuration and policy management**: Modern MDM solutions manage device configurations, such as setting role-based privileges or pushing out required OS and device patches. MDM solutions also allow enforcement of any mobile device policies a firm creates, whether for corporate or personal data and devices, such as permitting or denying device use internationally.

- **Self-service portals**: Popular with users and efficient for IT, self-service portals can be included in an MDM solution. Although law firm IT managers control the range of capabilities available, minimum offerings should include the ability to pre-enroll devices, view managed devices and perform a limited set of actions on them.

- **Flexible delivery options**: Many solutions offer both a traditional on-premises solution and a software as a service (SaaS) model. To get the best fit, evaluate both options.

MDM Standouts

Currently, no solution for managing mobile devices is one-size-fits-all. Instead, savvy firms carefully match the appropriate mobile device management (MDM) tool to their needs. Current options include:

- Absolute Software Manage MDM
- AirWatch
- BlackBerry Mobile Fusion
- BoxTone Mobile Device Management
- Fiberlink MaaS360
- McAfee Enterprise Mobility Management
- MobileIron
- SAP Afaria
- Symantec Mobile Management for Configuration Manager
- Citrix Zenprise MobileManager

Meeting Critical Objectives

If an employee loses a mobile device, the issue isn’t the cost of the gear. Rather, it’s recovering the trust and loyalty of clients whose confidential data might be exposed. MDM solutions let firms move the focus away from securing devices and toward securing the information residing on the devices — whether it’s case-related, financial or other client data.
Additionally, MDM solutions offer features aimed at assisting legal organizations with meeting compliance requirements (including the recently amended requirements in Rule 1.6 of the American Bar Association’s Model Rules of Professional Conduct as well as applicable state and federal laws such as the Federal Rules of Civil Procedure).

Security Policy Implementation
Swift consumerization has left many law firms without enforceable mobile security policies. For example, only 44 percent of company-owned smartphones and 38 percent of company-owned tablets can be scanned for malware, according to a recent Osterman Research survey.

The numbers fall to 10 percent and 9 percent, respectively, for BYOD devices. By adopting MDM, organizations can enforce policies that address such security challenges.

Remote Auditing
MDM solutions arm administrators with powerful device auditing tools, giving IT managers the ability to monitor and report on policy violations, such as user attempts to install blacklisted apps or visit blacklisted sites. Audit logs also enable the discovery of other items, such as configuration changes to devices.

Containerization or Sandboxing
In a BYOD world, it’s unreasonable to expect employees to use their devices only for business. Leveraging MDM allows IT managers to segregate business and personal traffic via so-called containerization or sandboxing. This functionality creates a secure container (or sandbox) for a firm’s data and applications, which is walled off from data and apps on the rest of the device.

Remote Device Wiping
According to the Osterman study, only 24 percent of personally owned smartphones and 21 percent of tablets can be remotely wiped at this time. For a law firm, that is an unacceptable risk. With MDM, administrators can remotely lock and wipe a missing device with a few keystrokes. More advanced solutions permit selective wiping, to enable the secure destruction of corporate property without disturbing personal data or applications.

Encryption
Mobile device encryption comes in many flavors. MDM permits administrators to set and enforce a minimum level of encryption, as well as identify what level of encryption exists on any given device.

Jailbreak Detection
It’s easy to find advice about how to disengage or “jailbreak” a mobile device from imposed security controls. MDM thwarts jailbreaking by automatically detecting unapproved configurations and disallowing the device until the situation is corrected.

Data Loss Prevention
Many solutions offer basic DLP controls such as monitoring keyboards, controlling which apps can be used and encrypting data. More advanced solutions link into document management systems or include content awareness to know when to disable features such as printing and forwarding.

Cloud Services Control
Whether it’s social media or document sharing, many cloud-based information services open the door to letting sensitive data escape. MDM solutions provide numerous avenues for administrators to limit cloud access or restrict it entirely.

Backup and Restore Management
MDM moves backup operations to a firm’s data center or a private cloud. This can help with greater data availability and increased productivity.

The Right MDM Solution
Despite the challenges of managing company and employee-owned mobile devices, there’s good news with respect to solutions. Legal IT pros have many excellent technology options for meeting the unique needs of their firms.

Product Selection Steps
As with any technology adoption, attention to detail pays off. Success lies in a thorough, requirements-based planning and evaluation process that includes the following:

1. **List objectives.** Group objectives into categories such as firm-level, device management and security needs.
2. **Prioritize objectives.** Within each category of objectives, determine which ones are primary, secondary or “nice to have.”
3. **Identify supported devices.** This list should include a survey of device types and OSs already in use, as well as those that employees may wish to adopt. Also, consider whether the firm will permit emerging categories of devices.

### MDM Rollout: 8-Point Checklist
- Develop a comprehensive mobile device policy.
- Begin communicating plans to rollout MDM to users.
- Inventory all firm-owned (and, where possible, employee-owned) devices.
- Devise a detailed rollout plan using a phased approach.
- Continue educating users as plans progress.
- Remotely configure devices and install apps during each rollout phase.
- Consider user feedback during each phase and make adjustments to subsequent phases.
- Provide user training to maximize self-service options.
4. Research available solutions. Conduct a market survey to identify a broad range of possible MDM options. Then, narrow the list to those solutions that offer features most closely matching the firm’s primary objectives.

5. Evaluate solutions on the short list. Determine which solutions most completely fulfill all of the firm’s identified objectives. If new considerations arise during the evaluation process, plug them into the objectives list.

6. Hold a bake-off or similar pilot. Request manufacturers provide a real-world trial. If a solution is an on-premises option, have the vendor provide a demonstration environment or request they install the solution in the firm’s test environment. Regardless, place several mobile devices under management and take time to experiment with the console.

7. Negotiate a contract. Review the licensing plans of the selected solution. Be sure to spell out any anticipated growth needs of the firm in terms of head count, international travel or number of devices per user.

8. Repeat steps. Whenever the firm needs to update, upgrade or build out its MDM solution, go through the steps again to ensure the adoption of the most efficient and effective solution available. Remember, lost productivity means lost billable hours.

Additional Considerations

During the research and evaluation phases, there are two other important functional considerations to explore:

• Delivery options: Like other software technologies, many of today’s MDM offerings can be delivered either as traditional hosted apps or via the cloud. For the highest level of control, traditional on-premises solutions remain king. The trade-offs are greater upfront costs and added complexity for data center administrators, but recurring maintenance costs are relatively small. For ease of administration and more flexible scalability, SaaS options are attractive. Solutions range from hosted versions of on-premises products to vendor-managed services. In the latter case, the provider performs all MDM tasks. The upfront capital costs of cloud-based options are relatively minimal; the recurring costs may be higher.

• Device management approaches: Manufacturers also fall into two basic categories in how they manage mobile devices. The agent model leverages traditional client/server technology, making its security capabilities the strongest of today’s approaches. The trade-off can be some intrusiveness to mobile device users, depending upon the specifics.

The API model relies on the application programming interface (API) provided by a mobile device’s OS. Although frequently the least intrusive to users, there’s a security trade-off because the controls are limited to those supported by each platform’s API.

Security 360

Like any security initiative, MDM provides just one layer of a firm’s defense— in—depth strategy. As Gartner Research Director Chae—Gi Lee points out, firms should “mobile enable” their IT infrastructures. To do so, a firm’s IT team should review and adopt (or upgrade) the following components:

• Wireless LAN infrastructure: With the latest generation of WLAN solutions, firms can establish access policies based on mobile device profiles such as user, device, applications and time of day.

• Network access control: For a firm’s wired network, NAC technology provides authentication capabilities that can dynamically assess the security posture of any wireless device attempting to connect. Using a NAC tool supplies a critical layer of security to a firm’s internal data.

• Mobile data protection: This technology complements MDM by ensuring notebooks and mobile media are properly protected.

• Enterprise policies and procedures: Well-defined security policies and procedures not only form the foundation of any technology deployment but also provide the building blocks for creating employee education materials. Staffers need clear directives that detail compliance requirements.

• User education and training: No matter how robust the security system, some users will seek ways around it if they think it’s in their — or the firm’s — best interest. To curtail such behavior, educate users about the reasons for each of the firm’s security measures and the consequences of breaking them.

Spurred by work mobility and the BYOD trend, law firms need to evaluate their situation and begin drafting detailed mobile strategies. Well—crafted policies protect both the firm and staff by clearly stating expectations and responsibilities concerning devices and the organization—owned and personal data on them.

To learn more about CDW mobility solutions, contact your CDW legal sales account manager, call 888.631.4239 or visit CDW.com/legal—solutions