MOBILE DEVICE MANAGEMENT: A WALL STREET I.T. PRO'S GUIDE

Successful financial firms deploy the right MDM to reduce risk and gain control of data in motion.

Executive Summary

No doubt some highly confidential financial documents and information gets passed around at capital markets firms. And more of it is being viewed and distributed via mobile devices.

Case in point: A recent survey by the advisory firm Aite Group revealed that nearly two-thirds (64 percent) of wealth management firms intend to pursue mobile initiatives from now through the end of 2014.

The desire to comply with staff preferences regarding mobile devices (both staff- and company-owned) must be balanced with IT responsibility to secure corporate data. To address the host of new challenges brought about by this wave, IT decision-makers are turning to mobile device management (MDM).

MDM solutions are designed to help keep data secure and achieve administrative efficiencies. They offer insight into the ways devices are used in capital markets firms while simultaneously enabling users to get their work done — anytime, anywhere.

TWEET THIS!

Table of Contents

The Situation

Fully 70 percent of banking-sector employees intend to purchase a tablet between now and the end of 2014, according to a recent survey by the research and analytics firm S&P Capital IQ. Of those, 32 percent will purchase their first tablet and 38 percent will upgrade to a newer version.

Naturally, bring-your-own-device (BYOD) initiatives are also making significant inroads. In fact, a recent report by the consulting firm PricewaterhouseCoopers shows that less than a third (28 percent) of financial services firms limit user-owned devices in the workplace.

Such mobile device enthusiasm is unsurprising, notes Bill Doyle, vice president and principal analyst at Forrester Research. "For financial firms, the mobile Internet presents a watershed opportunity to create more-continuous relationships with their clients," he says.

Yet, the explosion in device types and form factors also creates new challenges for the corporate IT staffs that must deploy controls across operating systems and applications. Fortunately, MDM solutions can fill the void.

Robust and mature MDM tools provide advanced capabilities to address a firm's unique operating environment. They are also designed to keep costs in check while simultaneously ensuring that employees stay productive.

According to a recent survey by the technology research firm Gartner, almost two-thirds (65 percent) of all organizations expect to adopt an MDM solution by 2017.

MDM 411

With the evolution of MDM tools, IT teams in capital markets firms can now more easily and centrally control smartphones, tablets and other gear. And the capability is available regardless of operating system (OS), hardware type or ownership status.

MDM programs typically function wirelessly to communicate with mobile devices and distribute apps. MDM programs — which can be provided via the cloud as software as a service (SaaS) or reside on premises using an appliance — support configuration, provisioning, monitoring, securing and support of mobile devices.

The IT team can establish device-agnostic policies from a centralized dashboard that will automatically synchronize on devices when users connect to the corporate network (whether onsite or remotely). In general, MDM functions include enforcing device security policies, performing remote troubleshooting, and deploying software and apps.

Strategic Features to Consider

MDM solutions offer a variety of robust features to meet the needs of investment firms:

- **Security management:** Because security is the primary reason for adopting MDM, security-related capabilities are the top priority for selecting the best fit.
- **Onsite or cloud-based:** As noted, many solutions offer both a traditional on-premises tool and a SaaS model. An organization's size often helps determine which approach would deliver the highest return on investment, with smaller firms opting for the cloud tools and larger ones taking the appliance route.
- **Cross-platform capability:** The era of fully supporting corporate-provided devices is waning, according to technology experts such as Gartner Research Director Terrence Cosgrove. Corporate-owned tools are "giving way to an era of 'managed diversity,' in which tiered support for employee-owned, consumer-class devices is the norm."

  This is one reason why many modern MDM solutions support a range of mobile OSs, including Apple iOS, Android, BES, Symbian and Windows Phone 8.
- **Asset management:** Today's MDM solutions allow remote control of all critical device management tasks, starting with inventorying gear and continuing through decommissioning devices.

  The same holds true for apps, which MDM solutions can detect, monitor and change. Other functionality includes pushing out apps and gathering statistics on apps — internal and external — that users adopt and utilize.
- **Configuration and policy management:** The latest device management tools streamline configuration tasks, such as setting role-based privileges and pushing out required OS and device patches.

  MDM solutions also enable enforcement of any mobile device policies that a firm creates, whether for corporate or personal data. They also can handle role-based downloading of apps to users' devices.
- **Self-service:** Popular with users and efficient for IT, self-service portals let users access apps approved by the corporate team. Although IT managers control the range of capabilities available to users, minimum offerings also typically include the ability to wipe, lock and locate lost devices.

Meeting Critical Security Objectives

The loss of a client's confidential data is a risk that a capital markets firm — or any business — can't afford. Further, the Financial Industry Regulatory Authority makes it clear in FINRA Regulatory Notice 11-39 that any business communication made via personal devices is subject to record-keeping requirements.

"From a practical perspective," says Henry Chien, analyst with the research and strategy advisory firm TABB Group, "Once a

personal device is connected to the enterprise, the firm has a regulatory responsibility to know essentially everything that occurs on the device."

MDM solutions let firms move the focus away from securing physical devices and toward securing the information residing on the devices. MDM capabilities include:

Security Policy Implementation

Swift consumerization has left many organizations struggling to enforce mobile security policies. For example, University of Glasgow researchers, using industry-standard forensic toolkits, found 11,135 digital artifacts remaining on 49 mobile phones re-sold on the secondary market. By adopting MDM, organizations can enforce policies that address this type of security challenge.

Remote Device Wiping

According to a recent Osterman Research study, only 24 percent of personally owned smartphones and 21 percent of tablets can be remotely wiped at this time. With MDM, it takes only a few keystrokes to wipe missing or decommissioned devices. More advanced solutions permit selective wiping, to enable the secure destruction of corporate assets while leaving personal property untouched.

Containerization or Sandboxing

In an environment of mixed corporate- and user-owned devices, MDM lets IT administrators segregate business and personal traffic by creating a secure container (or sandbox). This provides a method for walling off a firm's data and applications from the personal data and apps on the device.

Remote Auditing

Remotely monitoring and reporting on policy violations, such as user attempts to visit blacklisted sites or install blacklisted apps, is a hallmark MDM function. And MDM audit logs also enable the discovery of other regulated activities, such as changes to device configurations.

Encryption

Because mobile device encryption comes in many flavors, MDM permits administrators to set (and enforce) a minimum level of encryption, as well as identify the encryption controls that exist on any given device.

Jailbreak Detection

IT departments must be ever vigilant for users who try to disengage or "jailbreak" a mobile device from imposed security controls and thereby make enterprise data assets vulnerable to tampering. MDM can thwart jailbreaking by automatically detecting unapproved configurations and disallowing a device until the security controls have been reset.

Data Leak Protection

The use of data leak protection tools in the data center is not new, but their use for securing mobile information is. MDM solutions offer DLP controls ranging from the basics (monitoring keyboards, controlling allowable apps and encrypting data) to more advanced options (integrating with document management systems and providing content awareness to trigger the lockdown of features such as printing or forwarding of specified data).

Cloud Services Control

Many cloud-based information services make managing sensitive data tricky. MDM solutions can limit or prohibit cloud access based on policy settings.

Backup and Restore Management

MDM ensures that backup operations move information to a firm's data center or a private cloud when a device connects to the corporate network.

Getting a Wall Street–ready MDM Solution

Despite the challenges of managing company- and employee-owned mobile devices, there's good news with respect to the solutions now available. Consider the following suggestions as a guide for choosing the best product for a financial firm's specific environment.

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 steps:

1. Outline objectives. Group objectives into specific categories such as device management and security enforcement needs.

2. Prioritize objectives. Within each category of objectives, determine which ones are primary, secondary or "nice to have."

3. Determine 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.

4. Locate and narrow down available solutions. Research the market to identify a broad range of possible MDM options. Then, reduce the list to those solutions with features most closely matching the firm's primary objectives.

5. Evaluate short-list solutions. 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 outline.

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

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

8. Rinse and repeat. Whenever an MDM update, upgrade or build out is needed, go through the steps again to ensure the adoption of the most efficient and effective solution. Remember, lost productivity means lost revenue, so keep your solution current to maximize user capabilities while minimizing risk.

Additional Considerations

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

- **Delivery options:** 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. Also, recurring maintenance costs are relatively small. The trade-offs are greater upfront costs and added complexity for data center administrators.

  For ease of administration and more flexible scalability, SaaS options are attractive and 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:** The ways manufacturers manage mobile devices also fall into two basic categories. The agent model leverages traditional client/server technology, making its security capabilities the strongest of today's approaches. In return, there can be some intrusiveness to mobile device users, depending upon the specifics.

  The API model relies on the application programming interface 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 application programming interface.

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. This includes reviewing and adopting (or upgrading) the following components:

- **Wireless LAN infrastructure:** Use the latest WLAN solutions to establish access policies based on mobile device profiles such as user, device, applications and time of day.

MDM Options

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

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

- **Network Access Control:** Using NAC technology supplies a critical layer of security to a firm's internal data. On a firm's wired network, a NAC tool provides authentication capabilities for dynamically assessing the security posture of any wireless device attempting to connect.
- **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 form the foundation of any technology deployment and provide key building blocks for creating employee education materials. Employees need clear directives that detail compliance requirements.
- **User education and training:** Some users will seek ways around even the most robust security systems if they think it's in their — or the firm's — best interest. To curtail such behavior, educate users about the reasons for each security measure and the consequences of breaking it.

Regardless of a firm's approach, the need for a comprehensive mobile device strategy is clear. Perhaps analyst Chien sums it up best: "In a 24/7 connected world, the desktop is anachronistic. The consumer habits of Generation Y will shape the future of Wall Street, and financial institutions need to have an IT infrastructure that can adapt to and capitalize on them."

To learn more about CDW's mobility solutions, contact your CDW securities and investments account manager, call 888.706.4239 or visit CDW.com/financial-solutions.

TWEET THIS!

CDW PEOPLE WHO GET IT