# MOBILE DEVICE MANAGEMENT: NOT WHAT IT USED TO BE

Whether assigned or brought in ad hoc by staff, mobile-computing devices require MDM to protect enterprise IT assets.

## Executive Summary

The widespread proliferation of mobile devices puts unprecedented computing power and information at the fingertips of individuals throughout an organization. While offering advantages to both the enterprise as well as staff, IT shops struggle to deploy consistent controls across an array of varying software and device types.

Mobile-device management (MDM) software helps solve these issues by allowing IT administrators to gain cross-platform control of Apple iOS-, Android- and Windows-based devices. The strategy is to optimize the functionality and security of a mobile communication network while minimizing cost and downtime.

MDM solutions offer the ability to write security policies that are both platform- and device-agnostic, leaving the details of implementation to the MDM system itself. Other benefits include reduced support costs and business risks by controlling and protecting the data and configuration settings with advanced capabilities.

Moreover, MDM products offer insight into the ways devices are used in organizations. Administrators can monitor and control the applications installed on devices, monitor the use and transfer of information between mobile devices and enforce encryption policies for sensitive information.

TWEET THIS!

## Table of Contents

# The Mobile Stampede

From executives interested in displaying the latest tech gear to workers used to mixing social and work activities, personally owned mobile devices are flooding the workplace. And it's happening from the managerial suite to the factory floor, the principal's desk to the classroom, or the postmaster's office to the carrier on the street.

The consumerization of mobile technology has created an environment in which an organization's employees can purchase powerful mobile devices for their personal use at a very low cost. This home-based exposure to mobile technology logically creates new expectations for the way people work, whether they're in the office or on the road.

The variety of devices people use at home is also leaking into the workplace. Consider the impact on the enterprise of Apple's product line. As Apple's share of the consumer market grows, organizations are feeling more pressure from users who are familiar with those systems at home and want to use them for their office work.

And notebook computers aren't the only type of portable device that users are demanding in the workplace. Smartphones and tablets, that often get their first workout on a couch in front of the TV, are making their way to the office.

While the first reaction of many organizations may be to limit the flow of technology from the home to the office, that may not be practical because it can actually lower productivity. In the workplace, users generally aren't seeking new mobile platforms for their entertainment value. They truly want to increase their effectiveness by using tools that enhance their computing power.

## The BYOD Revolution

Not only do many users expect to have the same types of mobile devices at home and at work, they expect to use the same device for both. In short, staffers are requesting access to the devices and apps they want, while getting the enterprise data and connectivity they need.

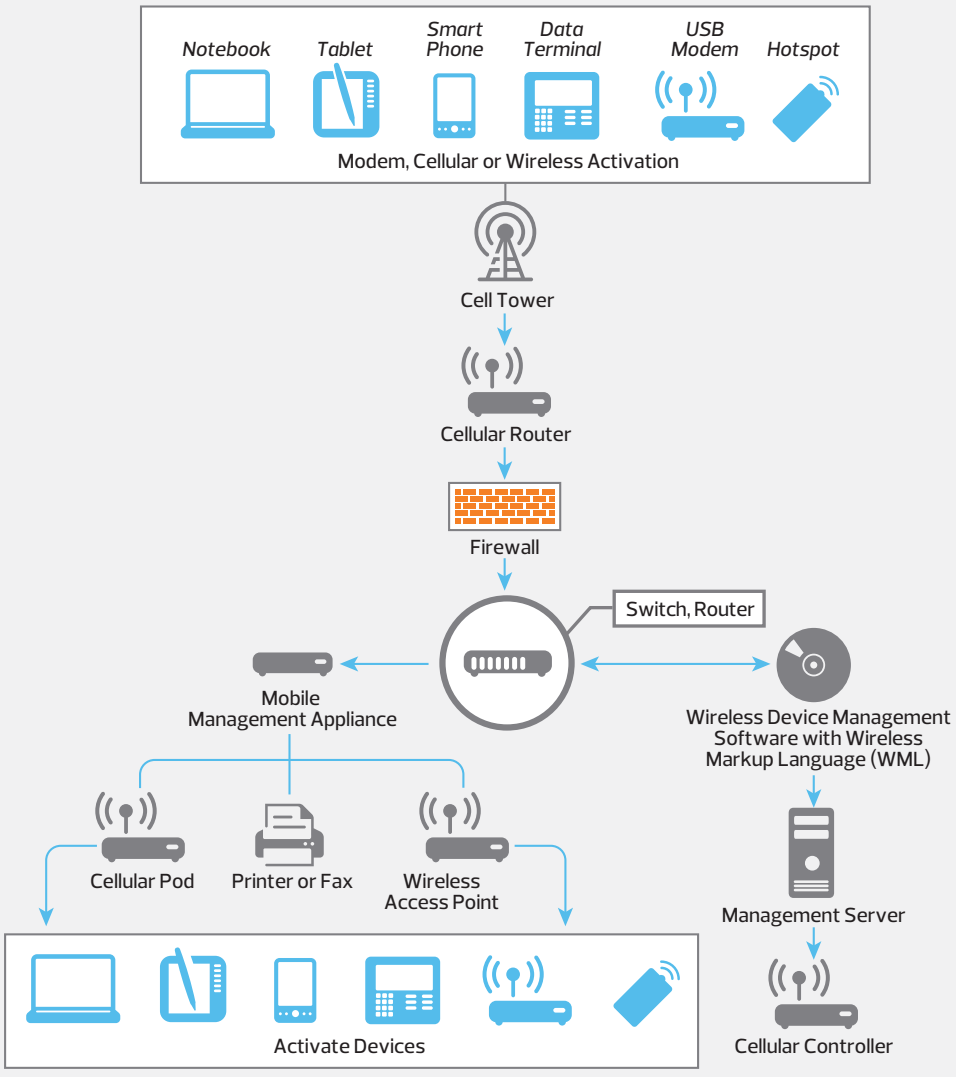
They want to simply purchase one device on their own and then use it to access both personal and corporate information. This growing trend is known as the bring-your-own-device (BYOD) approach to enterprise computing. And when adopted, it allows access to enterprise networks, which in turn become a mixed environment of organization-owned and employee-owned devices.

There are four main trends driving the BYOD revolution in enterprise computing:

**1. User satisfaction:** Tech-savvy staff want flexible work environments that let them transition easily between their work and personal lives. They want to be able to update their Facebook status in between e-mail checks and conference calls. Implementing a BYOD policy increases employee satisfaction by allowing them

### Mobility Solution

A variety of mobile devices is moving into the workplace.



to carry a tool for their job
that lets them to jump seamlessly between work and personal computing.

**2. Rapid technology advances:** With many enterprises on a four- or five-year equipment-refresh cycle, employees often want to get their hands on new technology faster and don't care if that means they have to open their own wallets to get it. BYOD can mean an organization's staff always have the latest technology without increasing the frequency of technology investments.

**3. An increasingly mobile workforce:** It's not unusual to walk into a local coffee shop on a Saturday afternoon and see a wide range of individuals with notebook computers, tablets and smartphones, sipping coffee and flipping through work e-mail. Accommodating the needs of mobile workers is a major trend driving BYOD adoption.

**4. Cost savings:** Quite simply, if employees bring their own computing devices to their jobs, the organization does not need to purchase hardware for them. In addition, the owner typically pays carrier charges for the device. Therefore, BYOD policies can wind up reducing hardware acquisition as well as carrier costs.

These four forces are driving many organizations to treat the BYOD trend as an opportunity. For example, Kraft Foods now offers employees a stipend to purchase their own computing devices, rather than purchasing devices for them. Employees who wish to purchase devices that exceed the stipend are free to do so out of their own pockets.

Other organizations adopting BYOD include CARFAX, Procter & Gamble, the Boulder Valley (Colo.) School District and the Veterans Affairs Department. These organizations also invested in security solutions that accommodate these policies.

## Mobile-device Management

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. Back then, it was easy for security administrators to create security policies from a centralized console and automatically push those requirements out to all systems that joined the network.

Mobile-device management solutions give administrators the ability to reassert control over the mobile devices attached to their networks, regardless of operating system, hardware type or ownership status. Administrators who leverage MDM can create device-agnostic security policies that go beyond current capabilities. For example:

The mobile data synchronization technology ActiveSync currently offers these management capabilities:

- Mobile device encryption requirement prior to network connection
- Enabled remote and select wipe capability on all mobile devices processing business data
- Allows or blocks devices using whitelists and/or blacklists

In addition, MDM software offers the following:

- Allows only applications approved by the administrator to be installed on devices processing business data
- Blocks business data transmission from a device managed via MDM to an unmanaged device or external e-mail address
- Allows convenient, efficient management across a number of devices on one control screen

Once the administrator defines these policies using the syntax of the MDM solution, the system handles conversion and deployment to all supported and managed mobile devices. The administrator does not need to know the configuration details for requiring device passcodes, for example, in iOS, Android, Windows Mobile and other platforms, because MDM handles the translation.

Using MDM levels the playing field for enterprises seeking to secure the diverse mobile-computing environments created by technology consumerization and BYOD policies. It gives

### Documenting a BYOD Relationship

The preferred approach to documenting a bring-your-own-device policy is to use a written contract listing the devices covered as well as specific details including:

- The types of information that may be stored, processed or transmitted
- The financial responsibility borne by users and the organization (if any) for the purchase, maintenance and replacement of BYOD devices
- The level of technical support (if any) that the organization's IT staff will provide to BYOD users
- The security controls (encryption, passcode protection, etc.) that the organization will deploy on the user's device as a condition of BYOD access to business information
- Any limitations in functionality that the user will experience on his or her device as a result of participating in the BYOD program
- The user's agreement to surrender the device to IT if required for an internal security investigation, response to discovery for a lawsuit or similar situation
- The user's agreement that the enterprise may remotely lock or wipe the device in the event it is lost or stolen, or if the user leaves the organization
- The user's agreement that remote wiping, if deemed necessary, may remove personal information from the device and that the user bears sole responsibility for backing up and restoring personal information
- Any other conditions of BYOD use imposed by the organization, based on security priorities

### Preparing Users for an MDM Rollout

It's important to remember that mobile-device management (MDM) is typically an IT-driven initiative. End users rarely clamor for new security controls on their devices because they fear — justly or unjustly — that the controls will hamper their ability to work effectively and infringe on their personal use of the devices.

Users don't always understand that MDM provides significant benefits to the enterprise by simplifying the delivery and management of mobile solutions to workforces of all sizes. Organizations planning a rollout should proactively communicate with users before deploying the software.

In addition to explaining the impact that MDM will have on users' devices, enterprises can take the opportunity to explain that MDM is a way of providing users with a means to safely access enterprise data from both enterprise-owned and personally owned devices. Users may also see benefits in the ability of the organization's IT staff to remotely configure their devices and install applications, relieving them of these administrative tasks.

IT professionals the confidence needed to allow the storage, processing and transmission of business data on devices they might or might not own.

## Critical Security Objectives

Security professionals who must develop MDM strategies are often motivated by one or two key requirements, along with a number of complementary objectives. In some cases, MDM projects are driven by compliance requirements, but the technology chosen is then leveraged to provide additional control over user behavior.

In other scenarios, MDM might be deployed as a solution to prevent users from installing unapproved applications. It may then be expanded later to include controls that protect against the theft of information stored on devices.

### Meeting Compliance Requirements

As with many security initiatives, compliance with the law, regulations or contractual obligations is often a key driver for implementations. For example, the Payment Card Industry Data Security Standard (PCI DSS) clearly requires that all devices used in the processing of payment card transactions implement security controls, including encryption and passcode protection.

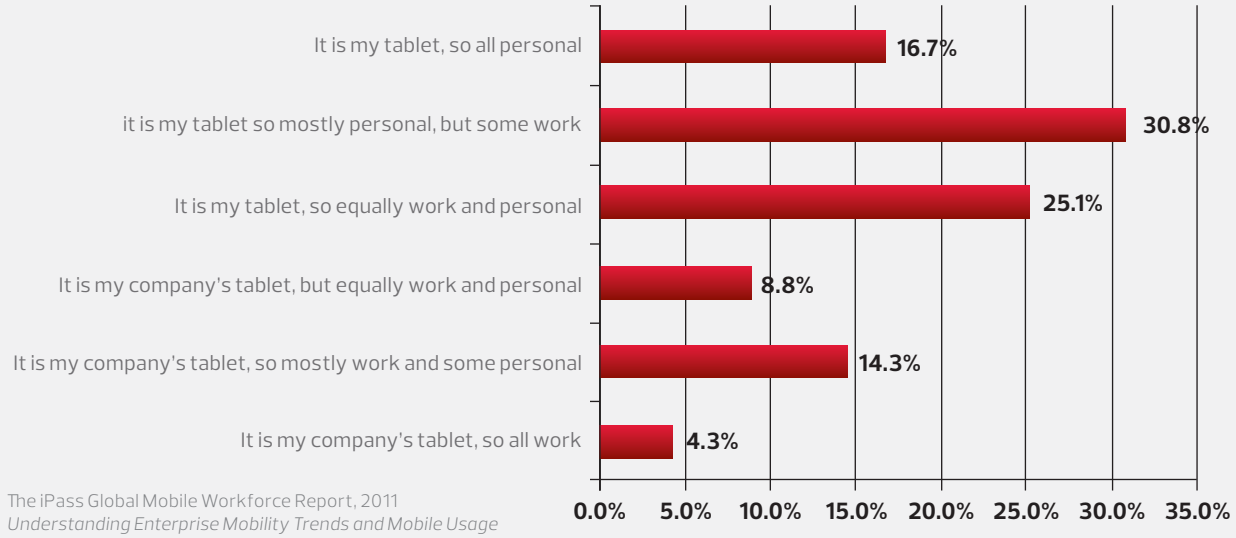
MDM solutions can enable enforcement of these controls. This allows security professionals to rest assured that devices remain compliant with the organization's obligations, even when those devices are used away from the enterprise network.

Electronic discovery, another common compliance issue, also can be complicated by the proliferation of mobile devices. Organizations that are involved in litigation or reasonably believe that they will become involved in litigation are legally required to preserve any relevant materials. Without MDM, administrators may find it difficult or even impossible to determine whether any mobile devices that employees might use contain materials subject to an electronic-discovery litigation hold.

### Implementing Security Policies

At this time, many organizations have yet to set up security policies aligned with the trend toward employee-owned devices. And if they have, such initiatives are often bare-boned and may lack a high degree of robustness. To cope with BYOD, what's needed is a set of well defined, consistent and properly applied MDM policies.

### Workers View the Tablet PC as a Personal and Work Device




The iPass Global Mobile Workforce Report, 2011
*Understanding Enterprise Mobility Trends and Mobile Usage*

Perhaps the most commonly used MDM tools are those that let administrators enforce an organization's security policies across a variety of platforms. As discussed earlier, MDM products let network management express security policies in clear terms and then consistently enforce those policies across all supported devices.

## Protecting Against Loss or Theft

Without an MDM solution, administrators have little recourse if a mobile device — regardless of who owns it — is lost or stolen. (Note, BlackBerry devices can be remote wiped.) They may interview the user to determine whether the device was protected by encryption or a strong passcode. However, these interviews often yield inconsistent results and are subject to the user accurately recalling the controls in place and honestly reporting them when it may not be in his or her interest to do so.

Through MDM technology, administrators gain proactive and reactive capabilities to protect an organization's data in the event a device is lost or stolen. From a proactive perspective, administrators can enforce consistent encryption and device security policies that reduce the chances that someone finding the missing device can actually extract data from it. And if a device is lost or stolen, administrators can react by remotely locking the device and wiping it clean of data, thereby removing any valuable information before a thief can exploit it.

## Sandboxing and Containerization

As far as security professionals are concerned, one of the most worrisome elements of the BYOD trend is the intermingling of personal and enterprise data and applications on mobile devices. Users want the ability to play Angry Birds and download a new app, while administrators want to ensure those applications don't gain access to corporate resources.

One approach to this issue — often used for enterprise-owned devices — is simply to prohibit the installation of unapproved applications. However, this can be difficult to enforce when an enterprise asks users to bring their own devices to work and use them for business purposes.

An alternative approach is to employ what are called containerization or sandboxing. These techniques build an environment within an environment on protected devices. They create a secure container (or sandbox) for business data and applications and wall off that container from the rest of the device's operating system.

When containerization is in use, MDM products allow enterprise administrators to configure the security controls surrounding the organizational container without affecting the rest of the device. Commonly implemented container controls include:

- **Preventing the export of data outside of the containerized applications:** For example, users running a containerized e-mail program might be prohibited from saving an e-mail attachment outside of the container.
- **Encrypting data stored within the container using enterprise-approved encryption algorithms:** This not only protects data if a device is lost or stolen, but it also reduces the risk that a noncontainerized application will be able to gain access to the data.
- **Allowing enterprise administrators to remotely wipe the containerized data and applications without affecting the rest of the device:** This is especially useful if an end user leaves the organization. Administrators can wipe out proprietary data without affecting the user's personal information.

The ability of MDM platforms to implement containerization controls depends on the deployment technique used by the platform, as well as the capabilities of each mobile operating system.

## Detecting "Jailbreaking"

Mobile devices have a number of built-in security controls that protect user data. Depending on the platform, these may include the restriction of applications to those installed through a centralized app store; limiting the capabilities of apps to access the underlying operating system; and preventing external connections to the device. Naturally, some power users dislike these controls, and the Internet is full of sites offering advice on how they can remove these restrictions by "jailbreaking" their devices.

As one might expect, jailbreaking mobile devices introduces a number of security concerns:

- Jailbroken devices may be able to bypass the security controls that would otherwise be enforced by an MDM solution.
- Vendor-issued security updates to a mobile device's operating system may not be available to jailbroken devices.
- Jailbroken devices may be able to run actions prohibited — for legitimate security reasons — on unaltered devices, including what's known as a secure shell or SSH daemon that accepts inbound connections.
- Jailbroken devices may also allow the "sideloading" of apps not allowed by the enterprise.

Without an MDM platform, IT administrators have no way of knowing if a user has jailbroken a device without physically inspecting it. But with MDM, IT managers can detect unapproved operating system configurations on altered mobile devices and can respond in a number of ways, ranging from removing enterprise data from the device to requiring that the user return the device for reimaging to a secure baseline configuration.

## Controlling Cloud Services

The consumerization of technology is not limited to the mobile-computing devices in end users' hands. It has also driven users to adopt cloud-based information services that give them ubiquitous access to information, collaboration

capabilities and social media. Security becomes an issue when users access such services via mobile devices, especially when the services employ unknown or unacceptable terms and conditions and the users are accessing enterprise data.

MDM platforms provide a number of ways for administrators to restrict the use of unauthorized cloud services. For instance, many cloud services require the installation of an app on the mobile device. The software distribution and restriction features of MDM products can limit users' ability to install these applications.

Also, containerization technology can allow users to install whatever software they wish on the nonenterprise side of the device. This will help prevent those applications from accessing enterprise data stored within the confines of the container.

### Additional Device Management

In addition to security functions, MDM platforms support a number of other management features. For example, many MDM platforms have device-provisioning features that allow administrators to push out configurations over the air without requiring users to visit the IT department. This is especially useful when managing a mobile workforce that rarely visits the home office.

MDM products also relieve administrators of some of the burden associated with tracking device inventories. Most feature asset-management functions that include linking employees and devices, tracking device age and replacement cycles, and monitoring the performance and technical characteristics of the device. Note, carrier expense and device lifecycle may also be provided by telecom expense management or TEM.

Finally, MDM platforms provide administrators with an easy way to push out enterprise applications to both corporate- and employee-owned mobile devices. Rather than asking users to visit an application store or download an application from a corporate server, administrators can simply push required applications to users over the air, improving the experience on both sides of the table.

### Mobile Device Recommendations for IT

- Consider adding tablets to the list of approved devices. While gaining popularity in the personal use market, they are now important business productivity tools.
- Make sure you pre-load the tablets with all necessary data security and productivity apps before issuance.
- Keep in mind, IT suppliers can add custom mobile apps as well as activations prior to device delivery.

## Choosing an MDM Solution

The goals of each organization's mobile-device management deployment will vary and may include one or more of the security objectives discussed earlier. Organizations considering an MDM solution should carefully evaluate the ability of various systems to meet their objectives.

Beyond that, MDM products differ in how they're deployed and how they actually manage mobile devices. There is no one-size-fits-all solution. Deployment and enforcement options will depend on the organization, its stand on usage models such as BYOD, and ultimately on its assessment of how users will react to and abide by MDM policies (see *Preparing Users for an MDM Roll-Out*).

### Selecting a Product

Organizations should conduct a methodical, requirements-based review of the MDM solutions available to them. One such approach might involve the following steps:

**1. Develop a list of enterprise security objectives.** Why is the organization planning to deploy MDM? Which are the primary objectives and which are secondary, "nice to have" objectives? And most important, what devices must be supported?

**2. Gather preliminary information.** Conduct a market survey of the available MDM solutions and identify those that, after preliminary analysis, seem to meet the organization's critical security objectives.

**3. Evaluate products that make the short list.** If some of the products are offered via the cloud, evaluation may be easy. Place a few mobile devices under management and experiment with the console. If this is not possible, ask if the vendor offers a demonstration environment that might be used in a similar manner.

**4. Deploy the selected product.** Develop an implementation strategy that rolls out MDM to both enterprise-owned and employee-owned devices. Organizations should carefully plan these deployments and communicate with stakeholders throughout the process.

### MDM Deployment Options

One of the major differentiators between MDM offerings is how vendors deliver the MDM service to organizations. There are two basic approaches:

- **Traditional on-premises MDM solutions:** These involve hosting hardware and software in the enterprise data center or virtual environment. This provides the highest degree of control, giving systems administrators direct access to configure the MDM software, as well as the underlying hardware and software platforms.

- **Cloud-based services:** MDM in the cloud offers a variety of deployment models. In some cases, these services are just hosted versions of traditional on-premise products. They relieve administrators of the burden of administering the application infrastructure while allowing full control over the MDM platform.

  In other cases, MDM management is pushed completely to the cloud as a managed security service, meaning administrators rely on the vendor to perform device-management updates and specific configuration tasks as opposed to completing them in-house.

In addition to considering the functionality of different MDM delivery options, organizations should also consider the financial consequences of these models. In the traditional approach, the enterprise typically incurs most of the expense as an upfront capital cost with a small recurring maintenance fee. With cloud-based services, there is typically a smaller capital investment, but the recurring operational costs are much higher.

### Device Management Approaches

MDM products from different vendors also take different approaches to the actual management of mobile devices. Different approaches may appeal to different enterprises.

In one model, the MDM solution leverages the application programming interfaces (APIs) provided by mobile OS vendors to perform device configuration. In an alternative model, the solution uses an agent-based approach that requires installing management software on each mobile device.

The API approach requires the least amount of intervention from users and administrators. It is appealing because it allows users to continue working with the same mobile tools they already use for e-mail, calendaring and collaboration.

In addition, devices can be easily provisioned for a managed environment without the installation of software. The downside of the API approach is that the security controls on each device are limited to those supported by each platform's API.

For end users, the agent-based approach to MDM is a little more visible. Products implementing this approach range from those that simply require installing a management client that runs in the background, to those that require users to perform all operations involving business data within a container that the agent provides.

This often means using the agent's specific e-mail and collaboration software, rather than the device's native apps (which may be the reason an end user selected a specific device in the first place). Typically, with an agent-based approach, user satisfaction may take a hit in order to achieve greater security.

## Defense-in-Depth Security

As with any security product, organizations deploying an MDM solution must remember that it is not a panacea to all the security issues raised by BYOD and other mobile-computing trends. Although MDM is a powerful tool, enterprises should consider it only one component of a well-rounded information security infrastructure that includes a variety of overlapping controls.

One supplementary control that organizations should consider is technology that restricts access to enterprise wireless networks to approved devices only. This may involve an approach as simple as requiring valid employee credentials when connecting a device to the organization's wireless network; or, it may use a more complex approach that allows connections only from devices that are either enterprise-owned or are part of a documented BYOD agreement.

Many organizations also use network access controls (NAC) as a way to assess the security of devices connected to enterprise networks. In addition to providing authentication capabilities, NAC can also dynamically assess the security posture of wireless devices. It can block devices from connecting to the enterprise network if they lack appropriate security controls, such as antivirus software with updated signatures, a current and patched version of a supported operating system and a functioning host firewall.

Finally, any well-rounded information security program must include a strong user education and training component. No matter how robust the security controls on a network, resourceful users often will find ways around those controls when they think it is in their best interest — or in the best interest of the organization.

For this reason, it's wise to invest the time and energy needed to educate users not only about the types of controls that will be implemented, but also about the rationale behind those controls. This is especially important for environments that intend to embrace BYOD. Users are much more likely to accept and use security tools when they understand why they're being imposed.

MDM products give security administrators an effective way to control the flow of sensitive business information across platforms and devices. From the user's perspective, data becomes available in many forms and on many devices, allowing greater productivity and better work/life balance. At the same time, from a security perspective, MDM controls remain constantly in place, following the data as it travels across users and devices.

# CDW: A Mobility Partner that Gets IT

When you decide that your computing environment and IT security program would benefit from a mobile-device management system, CDW has the experts and resources to get it up and running.

We offer a one-stop shop for integrated solutions via partnerships with leading MDM platform vendors including Absolute, AirWatch, BoxTone, BlackBerry Mobile Fusion, McAfee, Microsoft and MobileIron as well as companies like Citrix, Microsoft and VMware offering products that can help virtualize devices and applications in a mobile environment.

CDW has taken the guesswork out of buying MDM systems by pretesting best-of-breed solutions to match any budget. Our solutions include the most commonly deployed products on the market and accommodate a wide range of technical requirements and budget constraints.

Your CDW account manager and solution architects are ready to assist with every phase of choosing and leveraging the right MDM solution for your IT environment. Our approach includes:

- An initial discovery session to understand your goals, requirements and budget
- An assessment review of your existing environment and definition of project requirements
- Detailed manufacturer evaluations, recommendations, future environment design and proof of concept
- Procurement, configuration and deployment of the final solution
- Telephone support as well a product lifecycle support

**To learn more about CDW's mobility and MDM solutions, contact your CDW account manager, call 800.800.4239 or visit CDW.com/mobility**

TREND MICRO™

With the growing popularity of high-end mobile devices, many employees are opting to use their consumer-grade personal devices – such as PCs, tablets, and smartphones – in the workplace. Mobile Security is a fully integrated mobile-device management and security solution within a security framework that spans physical and virtual, PC and non-PC devices.

**CDW.com/trendmicro**

airwatch™ mobile device management

AirWatch's Mobile Device Management (MDM) solution enables you to manage large-scale deployments of mobile devices. Quickly enroll, secure, configure, monitor, manage and support corporate and employee-owned devices.

**CDW.com**

SOPHOS

Whether they're owned by employees or by your company, mobile devices on your corporate network need to be protected. We can help you keep sensitive data from leaving your company without getting in the way of employee productivity.

**CDW.com**

Symantec.

Symantec redefines endpoint security to address today's changing threat landscape – coupling proactive best-of-breed endpoint protection and endpoint compliance solutions to deliver more comprehensive security with greater control, at a lower cost, and with less complexity than competing solutions.

**CDW.com/symantec**

TWEET THIS!



CDW® PEOPLE WHO GET IT™