CDW PEOPLE WHO GET IT™

MDM: MANAGING THE EVOLUTION

The right mobile device management tools provide process improvements and efficiences rather than burdens.

Executive Summary

Mobility has moved quickly to the mainstream for organizations of all sizes and in all sectors. As the economy emerges from a long recession, enterprises want to become more efficient, reduce the footprint of their office real estate, attract the best and brightest workers and become more relevant to their customers and constituencies.

The old model of mobility has been transformed by a combination of powerful consumer devices, the technology to manage them as enterprise assets and new software development approaches. The ability to compute and communicate anywhere at any time, wirelessly on lightweight devices has transformed mobility.

From a software perspective, mobile apps provide a different user experience and greatly speed business processes and on-the-fly communications. Devices can run programs or act as mobile terminals, with instruction execution and data staying safely in virtualized data centers.

SHARE THIS WHITE PAPER

Table of Contents

2 MDM Trends: How the Market Is Evolving

4 MDM Product Considerations

5 MDM Evaluation Criteria

7 Mobile Services

8 CDW: A Managed Mobility Partner That Gets IT

But the power and opportunity of mobile technology comes with some serious challenges. Because devices are so light and portable, they introduce new security concerns, ranging from the simple loss of a device to the loss of critical business data or intellectual property.

Moreover, a growing number of employees and employers want to embrace bring-your-own-device policies. BYOD can make users happier and more productive, but it also brings fresh management challenges. These include accommodating several new operating systems, controlling telecom voice and data costs, and keeping track of devices and the state they are in with regard to application and security configurations.

These trends and challenges have given rise to a new class of software designed to enable secure, reliable and predictable deployment of mobility strategies. Mobile device management solutions have become the new enterprise IT resource management and control platform.

MDM packages incorporate functions covering the mobility lifecycle — device enrollment, configuration, app provisioning (from enterprise app catalogs), monitoring, policy enforcement, remote wiping or disabling, telecom expense management, disposal and replacement. MDM vendors are also adding the capability to monitor and manage desktop and notebook PCs.

This white paper will discuss the most important product characteristics and trends in MDM, helping IT managers to understand how their organizations can keep pace with mobile evolution.

MDM Trends: How the Market Is Evolving

Mobile device management, once just an add-on application for following small devices, has become a mission-critical tool that ensures far more than inventory control of mobile devices (although that remains an important function). Because mobility itself is transforming the computing models of a wide variety of organizations, MDM has taken on the function of coordinating all of the benefits of mobility itself.

One of the most important trends affecting MDM is BYOD, which seemed like an almost revolutionary concept when it first trickled into the market a few years ago. After all, employees have worked for decades under a system in which they were provided with an enterprise-issued PC, whose applications were provided and protected by the IT department. Most important, these workers in general didn't have administrative rights to their PCs and therefore couldn't install software — or even updates and patches — without IT intervention.

BYOD has proved attractive for enterprises and employees alike, but it turns the PC model on its head. Staff who bring their own devices have their own app collections aside from those the organization needs for them to use. In order to protect personal and enterprise data, personal and enterprise apps must be separated. To accomplish this, sandboxing (or containerization) has become a core MDM function.

BYOD also can introduce new operating systems into an organization's IT environment. Multiplicity of OSs has encouraged MDM developers to make their products more OS-agnostic and inclusive.

As enterprises have adopted BYOD, the practice has grown to include more than just smartphones and tablets. The consumerization of IT means many employees will want to bring a wide variety of their own devices: notebooks, ultrabooks, Mac devices — even Chromebooks and hybrid tablet/PCs. IT departments need a solution to manage all of these devices to maintain some orderly process for BYOD. A mobile device management system becomes the central repository for information about devices on the network, including fixed-location computers.

The BYOD phenomenon has not lessened the need for an enterprise approach to policy management. Thus, MDM has morphed into a suite of applications encompassing management of mobile products from multiple vendors. For example, Microsoft's Enterprise Mobility Suite is designed for Windows, iOS and Android devices. Likewise, BlackBerry's Enterprise Service MDM solution manages not only its own devices, but also iOS and Android, including multiple devices with multiple OSs for a given user.

Application, Content Management and BYOD

Mobile apps are designed to deliver information. As mobility becomes a mainstream computing strategy for the enterprise, delivery of content to and from mobile devices is rapidly becoming an important function of mobility management. At this point in the evolution of total mobility, mobile content management (MCM) is still often a stand-alone function, separate from mobile device management, that is offered by numerous niche vendors.

But MDM developers deliver MCM capabilities through enterprise mobile application management functions, such as app hosting, downloading and updating. MCM may be thought of as a technique for delivering the right enterprise content to the right mobile apps. Solutions that manage mobile content will adjust to certain conditions that affect mobile computing, such as:

Limited bandwidth: This is not an uncommon situation when devices move to certain Wi-Fi zones or when they operate in older cellular networks. By the same token, organizations want to have some limitations on content delivery to control cellular data costs.

Small screens: Device limitation can make some tasks unfeasible. For example, a busy PowerPoint slide might display well on a 7-inch or 10-inch tablet, but not be readable on a smartphone. Native apps often demand delivery of more specific information using fewer, simpler functions compared with browser applications.

End-to-end encryption: This security feature helps avoid the loss of data at rest on a device and in transit over the air.

Multiplicity of device OSs: This now-common issue requires the MCM to deal with more than three or four popular browsers.

The need for collaboration among employees working on documents also favors an MCM-specific solution or an enterprise content system with mobility extensions. This functionalist approach allows workers or business partners to edit spreadsheets, text documents, presentations, images and videos, often while viewing them simultaneously with others online.

MCM vendors are adding location-based functionality to content delivery. This capability can deliver targeted content based on a user's physical location as determined by a mobile device's GPS navigation system. Some content management systems also have the ability to push content from multiple data sources to mobile devices.

Some products let organizations manage disparate data sets and unstructured information in ways that assure legal compliance, sound record-keeping, satisfactory customer experience and worker productivity.

Big Data Optimizes Apps

Mobile apps and Big Data are technology trends that are both receiving plenty of attention from IT leaders. Perhaps it's no coincidence. Big Data success depends on combining not only large but also diverse data sources in ways that create valuable insights from that information.

Application programming interfaces (APIs) allow owners of data sources to make them accessible by apps. The federal government has roughly 100,000 data sets in machine-readable formats available to developers. Private data owners, such as Google and social media companies, also add APIs on top of their data sets.

For some enterprises deploying apps to their customers, blending in Big Data is crucial to keeping their apps relevant and engaging, according to mobility analyst Peggy Anne Salz, the author of *Apponomics*. She says organizations need to figure out how to use Big Data derived from customer or constituent usage patterns, which she calls data signals, to keep apps fresh and intuitive. That in turn helps build customer loyalty.

Major Changes in the MDM Market

In any fast-growing, fast-changing market, shifts in the vendor community can come at a breathtaking pace. As mobile device management grows and becomes more central to organizations' IT strategies, the vendor scene is changing. Established players are acquiring newcomers as the upstarts mature.

Some recent and noteworthy examples:

VMware acquired AirWatch in February 2014. VMware is partly owned by EMC, an IT conglomerate that makes products for enterprise storage, security/encryption and virtualization, among other IT sectors. The acquisition gives VMware a strong foothold in an MDM market that is expected to continue to grow at a rapid pace in the coming years. AirWatch is an early innovator in comprehensive MDM. It supports BYOD, enterprise app stores and device management for Android, iOS, BlackBerry, Symbian and Windows devices.

In late 2013, IBM completed its acquisition of Fiberlink. This vendor is best known as the publisher of the MaaS360 mobility management platform. This move complemented several years of work by IBM to build its cloud-hosting business; MaaS360 is a premier cloud-hosted MDM solution. The acquisition also complements IBM's comprehensive enterprise content management offerings as that functionality becomes mobile.

Citrix became a major MDM player when it acquired Zenprise in 2013. Following the acquisition, Citrix introduced its XenMobile platform, a comprehensive enterprise MDM solution that manages and secures data, applications and devices. The move establishes Citrix as a virtualization, telework and mobility platform provider.

These and other corporate moves reflect a fundamental shift in the IT industry itself. Vendors, CIOs and analysts have described a new era in computing. The old client-server model, with its fixed-location PCs on Ethernet LANs and notebook PCs with cellular or Wi-Fi cards, is being replaced by a new model of computing, marked by virtualization, use of third-party cloud services, ubiquitous wireless, mobility and data as a resource independent of specific applications.

Virtualization started with servers and is moving to storage, networking and desktop clients. By virtualizing its desktop infrastructure, an organization can let its mobile devices act as thin clients, with logic execution and data changes taking place in the data center rather than on the device.

The PC in all its forms is not disappearing. In fact, portable PCs come in more forms than ever — netbooks, ultrabooks and hybrid tablets, as well as traditional notebooks. MDM vendors are transforming their products into total endpoint management solutions, moving away from a purely mobile focus.

IT departments will need a way to set and enforce data access, application and other policies uniformly for users with more than one device — and that's rapidly becoming nearly all users. As this situation progresses, MDM will take over increasingly more enterprise IT management functions.

Use cases for Big Data and mobile apps are everywhere. In retail organizations, for instance, enterprise data on inventories and customers combine with location information in apps provided to customers.

For some developers, apps leavened with Big Data are more likely to attract advertising, turning the apps into an incremental source of revenue.

Big Data is also useful for internal, enterprise apps. Because Big Data analysis is becoming more important as a business intelligence strategy, it will move to mobile platforms as organizations deploy mobile devices.

Big Data applications bring together diverse data sources and, using a variety of technologies, can personalize content for users, provide predictive recommendations, detect anomalies and power analytical dashboards, among other functions. Few organizations are making optimal use of Big Data analytics, but many are finding ways to make use of Big Data and mobility for specific groups of users.

For example, executives on the go might want an alert to tell them about specific business developments in a native app on a mobile device when they can't access full dashboard applications on a PC. Field technicians might need a piece of information about a particular piece of equipment. In both cases, Big Data underlies the app, even if the app is selective in what it displays, depending on the context and the user's role.

MDM Product Considerations

Organizations should conduct a detailed analysis before choosing a mobile device management solution. With perhaps dozens of different products to choose from, each with varying features and capabilities, IT departments face a lot of choices and trade-offs.

The Emergence of MDM

Before the advent of MDM, enterprises adapted other platforms, such as enterprise application servers, to push applications out to devices, including mobile devices. As smartphones and tablets grew more powerful and became capable of mission-related applications, organizations needed more efficient ways to accommodate demand for BYOD that met their needs for security and cost control. MDM software emerged as a way of unifying a range of functions that the IT group must perform to enable the benefits of mobility while managing the risks.

For users, MDM mimics the processes with which they are familiar when using mobile devices in their personal lives. Using cellular or Wi-Fi networks, mobile devices can pull in data by downloading apps or content In turn, they can receive pushed material, such as app updates, email or text messages. This model translates to MDM, where an untethered device itself is the user's point of entry into the library of an organization's enterprise apps and services.

MDM software has some characteristics in common with enterprise resource planning (ERP) software in that it is a strategic platform for controlling significant assets, bundles many functions together and reaches into the farthest-flung parts of an organization, namely the mobile endpoints carried by employees.

Basic MDM Functions

Making an informed purchase decision of an MDM solution requires information. What's the criteria for selecting the right one? Start by comparing their basic functions.

Enrollment and authentication: These features bind the mobile device, the user and the organization. The IT department sets up the MDM to respond to each user according to a role-based set of parameters. To get started, users typically download an app, which leads to a sign-in screen for the MDM site. Employees use their organizational credentials, in most cases tied to an Active Directory or similar directory service.

App provisioning: This function occurs at the catalog. From there, a user downloads the container or sandbox, within which the apps corresponding to the user's role are placed. Most MDM products accommodate both custom enterprise apps and third-party apps with which the enterprise has made a licensing arrangement.

Security: This is a function both of the MDM itself and of the apps. The initial provisioning of a device includes creating the logical section within the device memory that keeps enterprise apps and data segregated from employees' personal content — the container or sandbox.

Beyond basic sandboxing, apps may be designed to enhance the separation. For example, many setups don't let users cut and paste to and from sandboxed apps, or they prohibit users from attaching enterprise documents to personal email and vice versa.

Some MDM solutions let IT managers limit the number of pages or files downloaded, and require passwords to access online files.

The mainstream mobile operating systems support encryption, some with software, some with Trusted Platform Module (TPM) hardware. MDM can make sure users encrypt their devices using built-in passcode functions. The passcode acts as the decryption key.

The MDM tool lets administrators restrict devices to designated Wi-Fi networks and also send an alert if they are jailbroken.

Remote access management: This provides an essential way for the IT department and network administrators to control devices. As an application, MDM gives IT admins a dashboard through which they can view the status of devices. More than simply monitoring devices, MDM lets the IT staff remotely

disable or even wipe a device that is reported lost or stolen. The same functionality lets IT staff reset or otherwise fix devices without having to physically handle them.

Many MDM publishers are adding the ability to view, provision and manage desktop PCs. In effect, they become total endpoint management solutions.

Mobile expense management (MEM): Some MDM solutions also can compile cost data for mobile devices — their usage of voice and data plans. MEM is an important component in total mobility management, as mobile service bills are now so complicated that they challenge organizations to understand them completely.

White Paper

Mobile Expense Management Made Easy



Read this white paper for information on how to get a handle on the mobile expense management process:
CDW.com/mobexpmngt

General management: These functions allow the IT team to establish settings for privacy, software usage and license monitoring. Administrators also can create and maintain app white lists, which compile a roster of apps that are approved for use, or blacklists of prohibited applications.

Enterprise data management: Depending on an enterprise's policies, the IT staff can configure the MDM solution to limit the drives, directories and files to which a given device has access.

Using containerization and controls on files, MDM can keep the distribution, sharing, editing and synchronizing of enterprise information within a secure end-to-end environment for both organization-supplied and employee-owned mobile devices.

Just as users have secure containers within their devices, they can also be given access to secure file space in the data center or cloud.

Before deploying any MDM system, IT staff must make the fundamental choice of whether to use a cloud solution or one hosted by the organization. Not all vendors offer both options.

MDM Evaluation Criteria

As with any enterprise software project, choosing a mobile device management system requires careful consideration of a long list of characteristics and features in order to find the right match for an organization. Here are several important characteristics of MDM to consider:

Scalability: MDM is not just for large organizations. Gartner research indicates that nearly half of MDM system purchases cover 100 seats or fewer, and the majority of sales are to organizations with 500 or fewer devices to manage. The same research indicates that organizations tend to have problems managing more than 500 devices without an MDM solution.

So as massive enterprises such as federal agencies and multinational corporations evaluate MDM solutions, they are evaluating products that can handle tens or even hundreds of thousands of devices.

Research conducted by the Enterprise Strategy Group found that a third of respondents reported difficulty with scaling MDM software up to large numbers of devices. In addition to the scalability with regard to the number of devices, IT managers should consider how an MDM solution can scale with the total number of apps deployed and maximum number of simultaneous virtual private network (VPN) transactions supported.

Mobile strategy fit: Mobile strategies vary. Some are outwardly directed, giving customers or constituents apps with which to access the products or services offered by the organization. That means internal, employee devices might be less of a priority. Other strategies focus on employees, giving them the tools to work anywhere and at any time. This often accompanies data center consolidation and a drive to reduce real estate.

Within an employee-focused strategy, enterprises must decide whether to supply devices for users or to support BYOD — a decision that will affect the choice of an MDM solution. How extensively mobility will reach in terms of functions and numbers of workers will become another decision factor. Some organizations want to move from a base of legacy mobile devices to a more diverse device population, driven by employee demand for BYOD.

Reporting capabilities: In thinking about the front end of mobile device management, it's easy to overlook the back end — the management reporting tools available to IT staff through the MDM dashboard. IT managers should look for MDM software that can deliver reports on basic device inventory, device population by operating system, status of devices in terms of apps loaded, file and download activity by groups or individual users, and cellular voice and data patterns of individual devices.

Reports should also cover enterprisewide trends such as total telecom usage. As the number of devices increases, enterprises need analytics on a variety of factors — coupled with alerts when activities exceed preset parameters — to effectively manage mobility.

Keeping data in the right container: Carriers and electronics stores deliver mobile devices in an unsecured state. Their native applications are designed to use common data and share updates. That's one important way they deliver a high degree of user acceptance. But most organizations want to avoid the mixing of employees' private data — contacts, photos, email, etc. — with enterprise data.

Yet within a secure container, mobility will be effective only if users have a successful experience. That's a central challenge of BYOD. Still, separating personal and enterprise data, and mobile content management generally, becomes the basic requirement for an MDM package. Some MDM solutions apply policies to existing apps through containerization or app wrapping; others supply high-grade proprietary email clients and browsers that mimic the functionality of popular apps.

Known single points of failure: MDM vendors won't advertise their SPOFs if they have them, but in any enterprise system the IT department must remain on guard for events with the potential to interrupt or shut down the operation. For cloud-hosted MDM software, IT staff should make sure the vendor has its own backup facilities if its principal data center suffers a failure. Organizations also should maintain backup connections with their software-as-a-service cloud providers.

For MDM hosted internally, the same practices for continuity of operations apply as for any enterprise service. Given the constant evolution of hacker exploits and malware threats to mobile operating systems, IT staff should not rule out the possibility of a device becoming a SPOF by infecting the enterprise network. Preventing this requires careful separation of secured and unsecured areas of device memory, attention to alerts and the readiness to execute remote disablement of connectivity on a device-by-device basis.

Customization: Organizations want MDM solutions that provide everything they need right out of the box, but often they have special needs or circumstances that require customization. As they evaluate MDM products, IT managers should consider how easily a product can be customized and how simply it can be integrated into the existing IT infrastructure.

Enterprise app store: Mobile strategies give rise to mobile apps. Considering that a mobility plan may entail three or more new operating systems and include both custom and public apps, the number of downloads available to workers can balloon quickly. MDM packages provide online app store functionality to organize and control apps.

The app store — some vendors call it an app catalog — should incorporate security settings so that apps download only into the secure container. It should enforce apps blacklists and ensure that all apps required for a given user are applied to the device. The app store also should support all of the operating systems supported by other MDM functions. A package may provide visibility and management to all of the major OSs but have an app store that is compatible only with two or three.

Enrollment groups: Nearly every user belongs to an organizational subgroup, depending on his or her job or function. An MDM's device enrollment and app provisioning, tied to the individual's directory credentials, can also assign group rights and restrictions to devices.

Other security issues: MDM vendors take varying approaches to mobile security. Some provide certificate and registration authority that integrates with the organization's overall certificate management, providing certificates at the device or app level. Others establish micro–virtual private networks between a device and the data center.

Many organizations look for products that provide Advanced Encryption Standard (AES) 256-bit encryption that meets the Federal Information Processing Standard (FIPS) Publication 140-2, or that restricts users' ability to cut and paste or back up to outside clouds. Other security considerations include establishing minimum password strength and automatic wiping of devices after a certain number of failed login attempts. An MDM solution should be able to push security policies, including data and file access, to the device level.

Mobility Success Starts with Policies

Mobile deployments require the attention not only of the IT department, but also of executive management, finance and user groups within an organization. A successful deployment demands a fully developed mobility policy. Elements of a policy include:

Device policy: Will the organization allow BYOD or provide devices to users — or some hybrid of these options depending on users' roles? If the organization provides the devices, the IT staff's job will be simplified, because the vendor can supply devices that are provisioned and ready to go. BYOD can be more demanding of the mobile device management system because users may be enrolling a wide variety of devices.

App policy: Which outside apps, or classes of apps, should be blacklisted or whitelisted? What is the decision process and who makes the final decision?

Security policy: Will devices be equipped with single sign-on for all apps? Will the organization retain the right to wipe an entire device, or only the secure container, if a security threat is deemed sufficient to justify such a measure?

Mobile Services

When mobility was simply a matter of syncing mobile phone email clients to an email server, the demands on the IT department remained reasonable. But now, the deployment of full mobility to large groups of users is a major technology and administrative undertaking. The IT staff may be burdened with other initiatives such as virtualization, data center optimization or a desktop hardware upgrade.

Mobility demands that an enterprise make many decisions before the first enterprise app is deployed, such as which functions will be mobilized; what the policies will be for devices, applications and data; and whether to host mobile device management software on premises or use a cloud provider.

The organization may need to decide among various priorities to determine whether to take on a mobility project in-house or outsource it to a third-party vendor. An outside vendor or consultant can speed policy development and then, at the organization's discretion, take on the technology components — in effect, offering mobility itself as a service. The decision to outsource, and thereby prioritize in-house IT resources for other projects, depends on answers to several questions. Among them:

- How closely is the mobility deployment tied to the core mission of the organization? Is the goal a total workforce transformation or just to bring more efficiency to a few key functions?
- Does the mobility strategy encompass customers and visitors to a website? Will the strategy entail development of public-facing apps?
- Is the organization ready for wide-scale mobility? Are user accounts virtualized? How many smartphones or tablets do employees already carry? Does the organization have good telecom expense management in place?

An outsourcing partner can handle the planning and policy elements of a mobility strategy, as well as the technical parts.

If the goal is to increase revenue or improve customer engagement through mobility, often an outsourcing partner has experience in these areas. Public-facing mobility best practices represent a moving target, and mistakes can be costly. An MDM partner can augment the IT staff's security knowledge base.

Similarly, a partner can deliver valuable help on internal-facing mobile deployments, providing shortcuts to proven best practices derived from experience.

In addition to policy and strategy development, an organization may also want to outsource specific tasks that, at an enterprise level, can take up a lot of time and work hours. These include:

Dealing with specific mobile-related technologies: This can include handling QR codes, developing mobile wallet systems, or adding geospatial information to applications as they are remade as mobile apps.

Developing, then implementing the security framework: The partner can perform tasks such as handling and managing encryption certificates, mapping enterprise data access rights and making sure policies are embedded in the MDM solution, tailored to various groups.

Performing mobile expense management: With hundreds or thousands of devices, each with its own voice and data plan (and perhaps multiple carriers), expense management can get out of control very quickly.

Implementation of a self-service portal: This resource allows users to select, activate, configure and deploy their own devices from an approved list.

Augmentation of the development staff with special expertise in mobile apps: Native apps generally work better for mobility, but not always. An experienced partner will know when an application rendered in a mobile browser can suffice, possibly speeding up deployment. Vendors can also manage app lifecycles, pushing updates to devices when functions change or device operating systems are updated.

Improving ROI

Outsourcing mobility services can improve the return on an organization's investment. How? It's a function of time.

Mobility requires upfront investment. The leadership of an organization wants to know whether that investment will pay off with better productivity, lower long-term costs or as a revenue improvement that outweighs the investment.

Speed of deployment and change management are two benefits of mobile device management outsourcing. By having a partner provide visibility into each device while handling the setup and administration of MDM, the IT team simply spends fewer work hours on the project. That means the benefits accrue more quickly, while the organization avoids delays and stays ahead of the learning curve.

The service provider can also handle device returns and repairs, deal with telecom expenses and provide mobility help desk support, further streamlining the mobility deployment process.

In short, as mobility inevitably becomes more complex, it will tax the time and other resources of IT departments. Given the growing popularity of software as a service (SaaS) and infrastructure as a service (IaaS) from cloud providers, mobility as a service (MaaS) is a logical next step.

CDW: A Managed Mobility Partner That Gets IT

The more complicated mobility management becomes, the stronger the case for acquiring mobility as a managed service. It might be a relatively simple matter to manage one device type from one carrier, but today, enterprises face myriad devices, carriers, plans, app development methodologies and BYOD flavors.

Through its managed mobility services, CDW can help.

That help can start at the planning stage of a mobility strategy. CDW brings a team of leading mobility strategists who can help any organization develop a unique plan, along with a roadmap for implementing it. Plan elements include policies for data, devices, mobile security, network requirements and mobile app development.

CDW will help an enterprise put the mobility plan into action. Our experts can help craft a BYOD policy that protects both enterprise data and employee privacy.

Once a mobility program is under way, CDW can help with ongoing mobile device and mobile app management from industry-leading partners. By hosting management services in the cloud, CDW's managed solution can scale along with an organization's requirements without the need for massive infrastructure investments.

CDW can deliver these services through a mobile management portal, customized to any enterprise. The portal lets IT staff procure devices, and offers visibility into and control over data and voice expenses, as well as providing worker support.

Employees can order their own devices, select carriers and perform upgrades, all according to the organization's policies. Devices arrive configured and provisioned within 48 hours.

The organization's IT managers receive reports and analysis of voice and data spending, so plans can be continuously adjusted for maximum efficiency. The dashboard also delivers information about device status and configuration, giving the IT team the tools it needs to troubleshoot, reconfigure, wipe and otherwise manage devices remotely.

CDW maintains a library of industry-specific apps. IT staff can also consult on custom mobile app development. CDW's partners have deep experience in a number of industries, and they understand the best practices in mobile apps.

Microsoft

CDW.com/microsoft

System Center 2012 R2 delivers unified management across on-premises, service provider and Microsoft Azure environments, thereby enabling the Microsoft Cloud OS. System Center 2012 R2 offers exciting new features and enhancements across infrastructure provisioning, infrastructure monitoring, application performance monitoring, automation and self-service, and IT service management. Benefits include the following:

- Enables the Microsoft Cloud OS by delivering unified management across on-premises, service provider, and Microsoft Azure environments
- Offers easy workload portability between Windows Server and Microsoft Azure
- Delivers optimal management for Windows Server environments that your critical business applications run on
- Can be easily integrated with existing enterprise management tools through the built-in web-service interfaces and Integration Packs

The information is provided for informational purposes. It is believed to be accurate but could contain errors. CDW does not intend to make any warranties, express or implied, about the products, services, or information that is discussed. CDW®, CDW·G® and The Right Technology. Right Away® are registered trademarks of CDW LLC. PEOPLE WHO GET IT™ is a trademark of CDW LLC.
All other trademarks and registered trademarks are the sole property of their respective owners.
Together we strive for perfection. ISO 9001:2000 certified
145519 – 140523 – ©2014 CDW LLC

CDW PEOPLE WHO GET IT