WHITE PAPER

CDW PEOPLE WHO GET IT

MICROSOFT MOBILE EMPOWERMENT

Greater productivity, security and management options are the gains from integrating mobile resources with the wider enterprise ecosystem via the Microsoft mobility stack.

Executive Summary

Every year, mobile computing becomes more important for enterprises. Employees insist on it; they have grown so accustomed to using portable devices in their leisure time that it's natural to extend mobility to the work environment.

Managed properly, enterprise mobility is also a boon for organizations. It provides workers with the tools to communicate and collaborate anywhere, with anyone, on any device, at any time. An effective mobility program removes time and location as barriers to work, improves users' ability to get work done and increases productivity and employee satisfaction.

Mobile applications are an important part of the productivity equation. The right apps, delivered securely, can streamline work processes and help workers remain productive, even during periods that used to be considered downtime, such as travel. All of this translates into a huge boost in productivity. According to Forrester Research, 47 percent of enterprises have experienced increased worker productivity after deploying mobile solutions due to faster decision-making, faster resolution of customer and internal IT issues, and improved customer satisfaction.

Table of Contents

However, all of these benefits require market-tested, secure mobile products that are fully integrated with an organization's networking infrastructure. Microsoft offers numerous products that can solidify an enterprise mobility strategy that is fully integrated with the network. Microsoft has steadily built its mobility stack into a mature, comprehensive set of tools that enables enterprises to confidently move forward.

Legacy IT Thinking

Today, all but the most forward-thinking organizations are still structured with the business side separated from the technology side. Even within the technology department, network management is separated from other areas of technology, including mobility.

While that setup may have worked in the past, the increasing presence of mobility in the enterprise — numerous studies show it to be among the most rapidly growing technology sectors — makes the separation of an organization's network infrastructure and its enterprise mobility technology a problem. And while mobility is largely a recent phenomenon, networks have been around for decades. Enterprises have figured out how to manage and secure them, but mobility changes the paradigm drastically, shifting the scope of the network and creating a number of security challenges.

Further clouding the picture is the emergence of bring-your-own-device programs that allow users access to data and IT resources on the organization's network via their personal devices. While it's challenging enough for an enterprise to secure devices that it has purchased, configured and managed itself, BYOD adds another level of difficulty, both from a technological and management perspective.

The network is a critical component to any enterprise mobility strategy. Without it, mobile devices can't access the data and applications they need, thereby stifling productivity. It's simply impossible to implement a mobility strategy without a networking infrastructure that supports it and is integrated with it.

One reason for the continued disconnect is that mobility initiatives often come from an organization's business unit, while networking decisions are generally made by the IT department. Thus, if an organization's chief executives want to mobilize its workforce, they will focus squarely on creating business applications and making sure that employees have access to those apps at any time, from anywhere, on any device, in a secure manner. But they

BYOD and Enterprise Mobility

The bring-your-own-device (BYOD) movement is no longer really a movement; it's a way of doing business for many organizations. According to Gartner, 38 percent of enterprises expect to stop providing devices to workers by 2017, and half will require employees to supply their own device for work purposes that same year.

The reasons vary, but cost is clearly a factor. In addition, allowing workers to use their own devices increases productivity, because they are more familiar and comfortable with them. This familiarity also translates into fewer IT troubleshooting issues and lowers employee resistance to using mobile devices for work-related purposes. Perhaps most important, BYOD is simply inevitable. Regardless of whether an organization allows it, many workers will use their devices for work-related tasks.

BYOD creates serious challenges for enterprises, especially around management and security. But the right tools, implemented correctly, can address these concerns. These include:

- **Mobile Data Management (MDM):** Software installed on each device or delivered via the cloud, through which organizations can control devices, enforce policies and encrypt data
- **Mobile Application Management (MAM):** Software applied to every application on a device that allows IT staff to lock down, secure and control only the organization's specific applications on a user's mobile device
- **Mobile Information Management (MIM):** Technology that keeps private data encrypted and allows only preapproved applications to transmit or access the data
- **Mobile Content Management (MCM):** Capability that allows users and administrators to share documents, presentations and video securely on mobile devices, also allows for remote updates and content erasure

While technology is critical to the management, success and security of BYOD programs, policies are just as crucial. Every organization should have a mobile policy, but many do not.

A mobility policy should include BYOD components and specify which devices (and operating systems) are supported. The policy should lay out password specifications, define which apps will be supported, explain the steps that will be taken if a device is lost or stolen, define who pays for the device, work-related apps and usage charges, and establish how data protection and security will be handled. The policy's security elements should include rules for downloading enterprise documents and limits on network and application access.

likely will be looking at the entire project from a business perspective, not from a networking perspective.

On the flip side, a network manager considering the enterprise's plans to focus on mobility may underestimate the bandwidth, security and services required to support users' devices and other needs. All of this can lead to problems, such as security issues involving access to enterprise data and other resources.

The key to avoiding these issues is to integrate the mobile strategy with the network infrastructure. Doing so provides better control over access, services delivered and cost. At the same time, it will improve worker efficiency and productivity and ensure that the organization has a single vision of enterprise mobility.

Microsoft's Traditional Strengths

For decades, Microsoft has been a leader in offering productivity and networking solutions, and it continues to innovate and improve in both of those areas. Microsoft's dominance is clear: More than 1 billion people use Office. And Office 365, the cloud-enabled version of Microsoft Office, is one of the fastest growing products in Microsoft's history.

What's more, 50 percent of Fortune 500 companies use Windows Azure, which stores about 10 trillion objects worldwide. Outlook has more than 400 million active users and is one of the most-used email services. And nearly half of companies plan to support Windows 8. What follows are some examples of how Microsoft keeps innovating with its traditional offerings.

Microsoft Windows

This offering has come a long way since the company rolled out its first incarnation in 1985, when it developed the first operating system based on MS-DOS and used the point-and-click interface method for the first time. Over the next several decades, Windows underwent many iterations and improvements, from Windows 98 to XP to Vista.

In 2009, Microsoft introduced Windows 7, which incorporated touch input technology for the first time. Windows 8 debuted in 2012, the first operating system optimized for the cloud and mobility. Today, Windows 8.1 offers a full array of applications and cloud connectivity available for virtually any device, personalization options, and the ability to view multiple applications simultaneously. Hundreds of millions of Windows 8 licenses have been sold since its debut.

Microsoft Office and Office 365

These products continue to push the envelope in office suites. Each of the individual components of Microsoft Office has continued to improve and add important features as well, including:

Word: Users can now embed videos directly into Word documents, and collaboration is easier with new features in the comment and markup section. Alignment guides help align objects more accurately, and the software offers numerous layout and table features.

Excel: A new start screen makes starting new spreadsheets easier and simplifies continuing work on existing documents. Recommended Charts help users more quickly decide on the chart type that will work best with their data sets. The new Flash Fill tool is designed to detect and anticipate user patterns and can extract and enter data more intuitively.

PowerPoint: New presenter tools include Presenter View, which allows users to see notes on their monitor while the audience sees only the slide. These tools also offer the ability to zoom in on or jump to a slide and to set up a monitor automatically. New design tools include more themes, smart guides for automatically lining up objects, improved video and audio support, and better color mapping. PowerPoint is also available for touch devices.

Outlook: The entire system is now faster. The new People Hub improves the contact section of Outlook, adding contacts' social networking updates. Other features include a message preview, attachment reminder, zoom slider and personalized themes.

OneNote: This note-taking application allows users to link notes to the original document or a calendar meeting, sync notes to audio and video recording, and embed Excel and Visio files.

Publisher: Publisher now allows users to insert pictures from online services and includes a touch mode. A new photo printing option saves document pages as JPEG files.

Access: This product, which helps users create desktop databases, now also allows them to build web-based database applications.

Lync Web Conferencing: Lync works with Windows 8, Windows Phone, iOS and Android. The Lync web app now has full conference support, allowing users who don't have the Lync client to join meetings with their browsers. New routing features improve connectivity and voice quality,

and Lync can now share with PowerPoint. The persistent chat feature saves the history of chat sessions, which allows users to join conferences and catch up quickly.

CDW and Microsoft: An Enterprise Mobility Match

Combining Microsoft's cutting-edge technology with CDW's enterprise mobility expertise is a great match. CDW's services include the following:

Mobility Pilot: CDW helps customers implement an enterprise mobility solution to support mobile devices. The pilot includes mobility design documentation and a mobility roadmap. The roadmap is based on discussions with senior-level stakeholders and CDW specialists. Together, they collaborate on a strategic vision for mobility's role in the organization.

Windows Intune Jumpstart: Jumping into mobile device management can be daunting. CDW takes the guesswork out by helping organizations plan, design and pilot Intune. The program can be designed as a full production-ready environment or a proof-of-concept deployment, depending on the enterprise's needs.

Microsoft Windows 8.1 Jumpstart: CDW helps bridge the gap by training an organization's IT staff on the latest tools and techniques for deploying and managing Windows 8.1, including Windows 8.1 Enterprise, Windows Server and System Center. The engagement also includes several days on security, as well as time dedicated to phone productivity and management, User Experience Virtualization, App Virtualization and a 50-day pilot.

Mobile Worker Productivity: CDW offers services that help improve the productivity of mobile workers.

Mobile Security: CDW provides training and service on full-volume encryption using Windows BitLocker Drive Encryption. This service helps enterprises make the most of the technology to ensure that sensitive information doesn't fall into the wrong hands if a mobile device goes missing.

Data protection using Microsoft's Active Directory Rights Management Services: Microsoft's AD RMS ensures that content shared among organizations or users is secure. It's also an ideal way to help meet and maintain regulatory compliance. CDW helps enterprises make the most of AD RMS by designing a detailed solution architecture and a proof of concept in a production environment.

Windows Azure

With its continued focus on the cloud, Microsoft is fully committed to Azure, its content delivery service optimized for media streaming. Microsoft continues to bring new features to Azure almost monthly. Some of the most prominent are:

Windows Azure Active Directory: This service provides secure access and single sign-on for cloud-based apps.

Windows Azure BizTalk Services: This cloud-based on-demand integration service allows organizations to securely build enterprise application integration (EAI) solutions and hybrid applications.

Windows Azure Traffic Manager: This feature helps enterprises ensure that applications are properly load-balanced.

Remote Desktop Services: RDS allows users to deploy and connect to applications, session desktops and virtual desktops. Continued innovations include session shadowing, which allows organizations to remotely monitor or control active sessions; online data deduplication, which significantly reduces storage capacity requirements; improved compression and bandwidth usage; the ability for display changes on the client to be automatically reflected on the remote client; and more administrator security options.

Microsoft's Maturing Mobility Platform

As mobile technology has evolved over the years and exploded over the past decade, Microsoft has steadily expanded its mobile platform. The path was clear: Organizations of all sizes were moving toward enterprise mobility at a staggering rate and needed a more comprehensive solution to achieve their goals securely. A report from the National Association of Software and Services Companies (NASSCOM) in association with the professional services firm Deloitte confirms this, noting that the global enterprise mobility market is expected to grow by a compound annual rate of 15 percent, to $140 billion by 2020.

Microsoft's first major enterprise mobility offering, Intune, debuted in 2010. First envisioned as an extension of System Center Configuration Manager (SCCM) for the cloud, Intune started out as a mobile device management (MDM) tool that runs in the cloud.

It works by installing a piece of software, called an agent, on every mobile device. The agent allows an organization's IT department to control the device's settings, such as disabling Bluetooth or a camera in keeping with enterprise policies, or sending a Wi-Fi or virtual private network (VPN) profile to the device so it automatically connects to the right access point with the right password. Finally, it can detect jailbroken or rooted devices that could potentially harm the network.

Microsoft continues to innovate Intune features with enterprise mobility in mind. Some of the newest features include remote lock and passcode reset for devices; the ability to configure an app so it can be displayed on an organization portal; and having Windows Intune Endpoint Protection installed by default.

As enterprise applications became more commonplace on mobile devices, Microsoft has added mobile application management (MAM) capabilities to Intune, which allow organizations to push software to devices and allow users to download approved applications from an enterprise app store, as well as the app stores from Microsoft, Google and Apple. Most important, MAM keeps business-related apps separate from personal apps, which is critical for security. The tool reports only on enterprise apps and data, leaving personal apps and data alone.

As the popularity of downloading apps continues to grow, Microsoft has increased its support for custom app stores as well as the offerings in its own Windows Store, which now boasts more than 140,000 apps. More than 4 billion apps and games have been downloaded from Windows Phone Store.

With the use of Intune growing steadily and the move toward enterprise mobility clearly on the rise, Microsoft upped the ante by unveiling its Enterprise Mobility Suite (EMS) stack, a comprehensive set of tools to help organizations achieve effective, secure enterprise mobility. EMS is based on Windows Server 2012 R2 with System Center 2012 R2 on top. In addition to Intune, Microsoft has added several important mobility tools to the stack:

Mobile Information Management: Already a feature of Active Directory, called Rights Management Services, this capability applies policies and encryption to the data stored on a device. For example, if an employee sends a colleague sensitive data in the body of an email or an attachment, that colleague wouldn't be able to forward it if MIM policies had been applied. MIM is application-agnostic; it doesn't matter where the data resides or which application is used. If MIM is enabled, the data is protected and secured.

Mobile Content Management: This feature enables workers to use their personal devices to securely access enterprise resources and services through multifactor authentication and evaluate and approve the device and the location. The main technology, called Workplace Join, allows an employee's own device to become an approved "known" device and enables it to use single sign-on for workplace resources and applications.

Web Application Proxy: This feature manages users' access to applications that run on an organization's servers. It serves as a barrier between enterprise applications and the Internet. Using Active Directory Federation Services, the service allows access to enterprise applications only to users with authenticated and authorized devices.

Work Folders: Essentially Enterprise File Sync for mobile devices, work folders work with MIM technology and can synchronize and keep files offline. This allows an organization to designate certain keywords, such as "secure" or "confidential," as candidates for rights management. With this feature, if a worker creates a document and uses one of those words, the system will find the keyword and apply rights management to it automatically during a file sync.

Enterprise Mobility by the Numbers

- Only 11 percent of end users access business applications from the office 100 percent of the time, according to the Cisco *Global Work Your Way Study*.
- By 2015, roughly half of employers will require their employees to use their own devices for work, according to the tech analyst firm Gartner.
- By 2017, 25 percent of organizations will have enterprise app stores, according to Gartner.
- About half of enterprises have implemented technologies to support mobile devices, with 48 percent using mobile device management and 47 percent using mobile application management, according to research conducted by the market research firm Vanson Bourne.
- Sixty-two percent of enterprises already have BYOD programs in place, according to TechRepublic's *BYOD Business Strategy Survey*.
- By the end of 2014, the average number of connected devices per knowledge worker will reach 2.8, up from 2.3 in 2012, according to Cisco's report, *BYOD: A Global Perspective*.

Hardware and OS Focus on Mobility

When it comes to enterprise mobility, Microsoft has also focused strongly on enabling both its hardware and operating system with the most effective features.

Windows Phone: On the hardware side, the Windows Phone, now bolstered by Microsoft's acquisition of Nokia, has made great inroads with its full feature set. Windows phones are ideal for a BYOD environment, with features for both casual users and road warriors, including hubs

for keeping groups of people, work apps and other elements together, as well as Skype, Live Apps, Office Mobile and cloud storage from SkyDrive. From a hardware perspective, many models come with high-performance cameras, high-resolution displays and powerful memory.

Surface tablets: Microsoft's Surface Pro tablets also are built with enterprises in mind. They come standard with Windows 8.1 Pro, 4th-generation Intel Core i5 processors and Office 2013 RT2, which includes touch-optimized versions of Outlook, Word, PowerPoint, Excel and OneNote. The tablets also have 200 gigabytes of SkyDrive cloud storage, a USB 3.0 port, a microSD card reader, front- and rear-facing cameras, up to 512GB of storage and up to 8GB of memory.

Windows 8.1 operating system: This includes a host of mobility, BYOD and security features. To foster mobility, Windows 8.1 now supports more VPN clients, and apps can now automatically trigger VPN connections. It also includes mobile broadband tethering, which can essentially transform a mobile device into a personal Wi-Fi hotspot. Another standout feature is Windows To Go, which allows users to boot Windows from a USB-connected external drive and enables users to move easily between devices.

BYOD-friendly features of Windows 8.1 Enterprise include Workplace Join, which allows users to work on their own device while still being able to access enterprise resources, as well as Work Folders and the Windows Intune MDM solution. In addition, the OS works with third-party MDM solutions.

Windows 8.1 also supports Miracast for streaming content from devices to a TV or projector. The OS also enforces multifactor authentication and conditional access policies. Other BYOD-related features include an enhanced virtual desktop infrastructure and the ability to print using either near-field communication or Wi-Fi connections.

When rolling out Windows 8.1, security was an essential consideration for Microsoft. Device encryption via BitLocker is now standard, and Windows Defender includes network behavior monitoring.

Windows 8.1 also offers native support for fingerprint reader technology, which allows users to secure folders through touch, and Assigned Access, which allows organizations or users to activate a single Windows Store application on the device. The operating system now supports partial wipes of devices, which is useful in BYOD cases in which a user wants to keep his or her apps and data safe from a wipe if the device is lost or stolen, or if the user leaves the organization.

Merging Microsoft's Networking Infrastructure with Mobility

Many enterprises are unaware that if they are using Active Directory and have System Center Configuration Manager, then they already have many of the components necessary to merge Microsoft's networking with its enterprise mobility tools. For example, System Center 2012 includes, among other features, Configuration Manager, Data Protection Manager, Endpoint Protection, Operations Manager, App Controller and Orchestrator. By adding the rest of Microsoft's EMS stack or combining its offerings with existing technology, organizations can be sure that the entire stack is fully integrated and supports both Windows and non-Windows devices and apps.

These solutions together make it much easier to manage devices running any operating system — including Apple iOS and Android devices — from one environment. Integration is also critical for security, allowing an enterprise's IT department to deploy certificates, profiles and settings consistently, and also implement remote wipes, remotely lock devices and issue patches. Finally, full integration allows organizations to easily monitor resources, change settings and provide a consistent and secure experience for the entire infrastructure and its users.

Because many enterprises already have Microsoft's tools and network infrastructure running in their environment, a shift to full enterprise mobility integrated with networking, all on a Microsoft platform, makes sense from a licensing perspective. Often, it simply takes adding a handful of new tools to create a complete solution.

Finally, the Microsoft ecosystem has been designed from the ground up to be consistent in terms of look and feel. That eases the learning curve on new Microsoft technology for both employees and IT staff.

Putting It All Together

While integration of the network infrastructure and mobility is a critical task, it can be difficult to get started, even with the right technology. Here are some tips for making it go smoothly:

Establish mobility requirements early in the project. Whether an organization does this by gathering a group of stakeholders and users together or by enlisting a third party, this has to be the first step. The requirements should encompass everything that each department may need over the next three to five years.

These requirements can be both aspirational (creating new revenue streams or improving the availability of essential employees) or technological (allowing users to work remotely in a more efficient and secure manner or beginning a BYOD program). This is also the time to specify non-negotiable security or access requirements, as well as a timeline and budget.

Why Microsoft EMS?

Microsoft's Enterprise Mobility Management solution is a comprehensive approach to enterprise mobility, based on Windows Server 2012 R2 and System Center 2012 R2. With this mobility stack deployed, enterprises can improve on the following:

- **Application delivery:** EMS allows administrators to deliver a single approved application to all users' devices in the most efficient manner for each specific device, such as streaming through App-V, via Remote Desktop Services.
- **Device management:** The Windows Intune component of the EMS stack ensures that all enterprise policies are enforced across both mobile and on-premises equipment.
- **Application management:** Through Intune, EMS ensures that only approved applications can be downloaded to an employee's device.
- **Information management:** This rights management technology applies enterprise policies and encryption to data stored on a device.
- **Virtual desktop management:** The Configuration Manager tool manages all client desktops, virtual desktops, thin clients and mobile devices.
- **Endpoint protection:** Configuration Manager provides full endpoint security, including malware protection and identification. It also provides visibility into noncompliant systems.
- **Compliance and settings management:** This tool allows managers to set and enforce a "desired configuration state" for devices.
- **Software update management:** This capability lets IT administrators deliver and manage updates of not only Microsoft products, but also third-party applications, hardware drivers and system BIOS to mobile devices, desktops, notebooks and servers.
- **Power management:** Client power management tools help optimize power settings for mobile devices.
- **Operating system management:** This feature distributes operating systems to all devices across enterprise networks.
- **Client health and monitoring:** A console shows the health of all devices and activities and alerts the manager of problems.
- **Asset intelligence:** This capability provides continuous visibility into all hardware and software assets and usage.
- **Inventory:** Configuration Manager can keep a running inventory of all hardware and software used by an organization.

Decide who is in charge of each part of both the project and the final result. In some cases, the network manager may take a primary role. In others, it may be an IT manager dedicated to enterprise mobility.

Evaluate technology. Does the IT shop want to work around existing solutions? Does it want to start from scratch? IT managers should make sure that the technologies it considers meet the organization's requirements for flexibility, scalability, security and manageability.

Develop a governance policy. Although it might seem counterintuitive, it's important to create and communicate this policy before implementing new technology. That way, users and executives know what to expect. Nobody likes surprises.

The policy should cover both enterprise-issued and employee-owned devices, as well as device management and lifecycle. The policy should spell out restrictions on business networks, along with application and data access, and steps that will be taken if a user leaves the organization or loses a device. It should also include policies that must be followed to ensure compliance with appropriate mandates.

Implement mobility in phases, one piece at a time. This practice lets the IT department prove to stakeholders and users that the plan is working before moving on to another phase. This approach applies not only to technology (for example, getting MDM working before moving to MAM or MIM) but also to rolling out the technology one department at a time.

Test after each phase, and make sure that stakeholders and users are satisfied. This step is essential to finding out what works (and what doesn't) and ensuring that security is airtight.

Finally, organizations should consider bringing in a third party to help from the evaluation phase through requirements, implementation and testing. By working with a third party that understands the mobility roadmap and can evaluate an enterprise's specific needs and requirements, stakeholders will have the highest degree of confidence that the approach taken is the right one.

Enterprise mobility is clearly here to stay, and organizations don't have much choice when it comes to jumping on board. Finding the right technology and the right partner are key in making it work.

The (Near) Future of Enterprise Mobility

Technology is moving at a rapid place, and mobility is perhaps moving faster than any other sector. By having the right technologies in place and the right mindset, organizations will be well positioned for what's ahead. Advances are likely to include some combination of the following:

More management choices: A growing cadre of professionals are considering a cousin to BYOD: corporately owned, personally enabled (COPE) devices. This approach manages personal data differently than BYOD. With BYOD, workers own their devices, but with COPE, organizations provide the devices to workers and allow them to be used as their personal devices, with their own data and apps.

Some believe that the COPE model gives enterprises more control, because they can choose the carrier, the devices and the apps to be preinstalled. Organizations can subject the devices to scheduled or unscheduled malware checks and send warnings about specific apps. COPE is expected to gain many converts in the coming years.

Augmented reality: It may seem like science fiction, but augmented reality, in which a view of the real world is supplemented by input generated by a computer, can be a very useful tool. The technology combines digital and virtual information, including video, audio, 3D content and computer-generated images in real time. With 2D and 3D augmented reality-enabled apps, organizations can improve the user experience in a wide variety of sectors, from virtualized product experiences for customers to navigation and location-based advertising.

Wearable computers: Wearable computers are already here, and the market is set to grow by more than 40 percent through 2018, according to Transparency Market Research. Many enterprises have use for these hands-free devices, which offer greater facilitation of information and collaboration, and more detailed guidance for intricate manual tasks in areas such as field service. Use cases include better navigation of physical environments and support for military and intelligence operations.

To learn more about combining Microsoft technology with CDW's enterprise mobility expertise, contact your CDW account manager, call 800.800.4239 or visit CDW.com/microsoft

---

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:

- Offers easy workload portability between Windows Server and Microsoft Azure
- Delivers optimal management for Windows Server environments that critical business applications run on
- Can be easily integrated with existing enterprise management tools through the built-in web-service interfaces and Integration Packs

SHARE THIS WHITE PAPER

CDW PEOPLE WHO GET IT