CDW PEOPLE WHO GET IT

THE TOOLS TO POWER A NEW WAY TO WORK

Mobile devices and software deliver the capability for workers to remain productive in new ways and places.

Executive Summary

Conference calls from airport lounges. Business deals over coffee. Work orders completed, printed and signed at project sites. Thanks to the ubiquity and growing sophistication of mobile devices, work is increasingly conducted outside of the office. Whether employees use personal or enterprise devices, they have grown accustomed to doing work anytime, anywhere.

Few need to be convinced of the value of mobility. The potential for both productivity and work/life balance is clear. However, the market is flooded with an array of smartphones, tablets, phablets (a smartphone with a tablet-sized screen), notebooks and peripheral mobile equipment, not to mention tools to manage and secure them. While devices can usually run on their own, complexities often arise when they are paired with other hardware and software. What's more, managing a complex mobile infrastructure can be labor-intensive and costly.

Microsoft has addressed this complexity by compiling a comprehensive suite of mobile products designed to provide employees with limitless mobility without compromising security. It offers tools that let administrators set parameters regarding how mobile devices are used and what happens to the data they access. In addition to Surface tablets, Office 365 and System Center, Microsoft now offers the Enterprise Mobility Suite, which includes Intune, Azure Active Directory Premium and Azure Rights Management.

Table of Contents

As effective as they are on their own, these best-in-class tools are designed to work together, making the suite easier to use and manage than many stand-alone mobility products. They integrate seamlessly with the Microsoft tools that companies have used for years, and their integration gives users added features and benefits. Rather than devote months to implementing new infrastructure, the organization can integrate Microsoft's mobility suite within days and know that it has comprehensive coverage.

A New Way to Work

Among all the technological changes and new trends, mobility stands out. More than two-thirds of IT professionals say mobility is likely to affect their work the way the Internet did 20 years ago, if not more.

The mobile revolution is great news for businesses. Mobile devices can boost worker efficiency and productivity. Users can finish projects from home, communicate with colleagues while traveling and keep the business running even when disasters close the office. They can upload notes and forms directly to the corporate server rather than gathering data in the field and transcribing it back at the office. They can even take photos and scan documents from the road.

As many as 89 percent of workers surveyed say that mobility makes them more efficient on the job, which extends beyond work hours. Because employees have smartphones and tablets with them wherever they go, they check email, communicate with clients and colleagues and work on projects even when they are not on the clock.

What's more, 80 percent of professionals feel the flexibility in work hours is a good thing. Mobile devices also give them the flexibility to do their work when and where it is most convenient, rather than being chained to a desk from 9 to 5. Mobile technology also allows users to take care of personal responsibilities during the day (such as responding to email at the doctor's office or taking a work call while commuting). That flexibility, for many, equates to a better work/life balance.

With mobile technology, users have access to a seemingly endless supply of applications to help them work better, smarter and more efficiently. More than half of workers say that apps help them do their jobs better. With a smartphone in hand, a user can access document scanners, project management resources, dictation tools and contracts wherever they are. Two-thirds of workers say their productivity would be even higher with more apps.

These apps help staff to effectively communicate and collaborate with colleagues and clients. They provide workers with 24/7 access to email, messaging tools and document-sharing services. Microsoft's Office 365 brings together the best-in-class tools in each of these categories. A project team with members scattered across the globe can co-author a document in real time and video conference daily, staying just as connected as if they were down the hall from one another. An employee who travels during an important presentation can participate via smartphone or tablet while waiting for a connecting flight.

HOLE IN ONE

As Calloway Golf's business grew from a boutique firm to one of the world's leading manufacturers of golf products, its IT infrastructure grew to keep up. Eventually, it grew out of control.

In addition to the main data center in its Carlsbad, Calif., headquarters, the company had data centers scattered across the country, many of them underutilized. The company also was challenged to manage and protect the 350 Windows-based notebooks used by employees and 130 tablets used by outside sale representatives.

Calloway decided that migrating to the cloud could simplify its architecture, cut infrastructure costs and make the company more agile. IT decision-makers turned to the Microsoft Azure cloud platform. Not only is Azure a comprehensive solution, but Calloway's IT team is already trained in Microsoft tools, which made for an easier integration of Azure into its existing systems.

Calloway also implemented Microsoft Intune with Microsoft System Center 2012 Endpoint Protection to manage and secure its notebooks and tablets. The system worked so well that the company decided to upgrade to Microsoft System Center 2012 R2 Configuration Manager (SCCM) to manage its 850 desktops.

Not only can mobility make workers more productive, it can boost morale as well. Since so many people use mobile devices in their personal lives, it's natural for them to use the same devices on the job. Most workers appreciate employers that equip them with the powerful mobile tools they use in their personal lives.

While the advantages of mobility are clear, the objective for organizations is to provide employees with the tools to do their jobs anywhere on any device without losing control of their infrastructures. With the influx of additional devices and applications being used by staff, this is a challenging goal. By implementing a suite of tools to deploy, manage and secure both the on-premises and the mobile infrastructure, organizations can stay in control and reap the rewards of mobility while minimizing risk.

Surface Tablets

Despite the benefits of mobile devices, many users feel most mobile operating systems are not robust enough to replace a computer. As a result, many use desktops or notebooks in the office and tablets while on the go. Consequently, organizations end up purchasing and supporting multiple devices per user. Staff must also ensure their devices are synchronized properly, or that files are transferred so they can be accessed on the right device at the right time.

The Surface Pro 3 and Surface 3 tablets help to solve these problems. They offer the portability of a tablet with the operating system of a desktop computer. Users no longer need different devices for different tasks. Both tablets come preloaded with

Microsoft Windows 8.1 Pro — and include a free upgrade to Windows 10 — giving users the capabilities of a full-sized computer in a tablet that weighs less than 2 pounds. They are exceptional mobile devices — thin and light, with a full operating system.

The Surface Pro 3 has a 12-inch screen, weighs 1.76 pounds, has a battery life of up to nine hours and is Wi-Fi enabled. By comparison, the Surface 3 screen is 10.8 inches, it weighs 1.37 pounds, the battery lasts up to 10 hours and it has Wi-Fi and optional 4G LTE technology. Both tablets are completely portable, yet they can instantly transform into desktop systems in the office. They slide right into a docking station, which can be connected to an external monitor (the Surface Pro 3 can connect to two monitors). Their ports — a full-size USB 3.0, microSD card reader and Mini DisplayPort — also make it easy to connect to other peripheral devices and transfer files.

In addition to running the full Windows 8.1 Pro operating system, Surface tablets have the power and performance to run thousands of sophisticated applications, including the popular Microsoft Office suite. The Surface Pro 3 has a fourth-generation Intel Core processor, providing fast performance, and up to 512 gigabytes of memory with 8GB of RAM. The Surface 3 includes a Quad Core Intel Atom x7 processor with up to 128GB of storage.

Based on how they prefer to work, users can choose a detachable keyboard or bright, responsive touch screens. The tablets include built-in kickstands that set in multiple positions. They also include the Surface Pen, a stylus that feels like a high-end fountain pen. The Surface Pen allows users to annotate reports, collect signatures and create sketches.

Because the tablets are designed by Microsoft, they are tightly integrated with software such as OneNote and Office 365. For instance, even if the tablet is locked or asleep, a user can simply click the Surface Pen, and the device will wake and open a new OneNote page. Another click saves the file and syncs it to the cloud.

OFFICE SPACE

Office 365 provides enterprises with cloud-based versions of Microsoft's popular Office applications, and cost savings as well. But those aren't the only reasons the suite makes sense for business:

- **The benefits of the cloud to users:** By storing files in the cloud, Office 365 allows users to access their work anytime, anywhere. With 1 terabyte of storage per user, enterprises have no risk of running out of space. Office 365 synchronizes data across devices, so users no longer need to transfer or email files. A project manager can create an Excel file on his notebook while meeting with his team in the conference room, then access the spreadsheet from his tablet at home that night.
- **Enhanced collaboration:** Using Office 365 cloud-based collaboration tools, a manager can access team members' calendars, send instant messages and participate in Skype video conference calls during which the entire team can access and edit a single document together. They can also use SharePoint to give people outside of the company access to large files. For instance, they can access and co-author a PowerPoint presentation, share it with a contractor to edit it, then submit it to a client when it is finished.
- **Maintaining Office applications:** Since Office launched in 1988, Microsoft has set the bar with regard to office software. The biggest challenge has been managing different versions of Office applications enterprisewide. With Office 365, applications are automatically updated, so users are always getting the benefit of the latest version.
- **Email and calendar:** Office 365 syncs email, calendars, tasks and contacts as well as files. Enterprises can create customized email formats and domain names for email accounts and access advanced features such as eDiscovery to deliver and store electronic data that can be used as legal evidence. Office 365 can send messages up to 25 megabytes and includes 50 gigabytes of storage per user, so users can save old email messages without fear of running out of space. It also includes simple user and administrator email management tools and best-in-class anti-spam and malware protection.
- **Security:** Office 365 provides physical security measures to keep networks and data centers secure. For further security customization, Microsoft provides additional controls: Rights Management services requires proper credentials in order to access files, Office 365 Message Encryption lets users encrypt email, and data loss prevention keeps sensitive data from getting into the wrong hands. All three controls can be combined for stronger security.

  Physical security measures include multifactor authentication, biometric readers, motion sensors, video camera surveillance and alarms to keep Microsoft's data centers secure; logical security steps, including perimeter vulnerability scanning and intrusion detection; data security, such as encrypting data at rest and in transit; and security monitoring.
- **Availability:** The benefits of Office 365 extend as much to IT administrators as they do to users. Not only does Office 365 have easy-to-use management controls, but Microsoft assumes the burden of keeping systems running. IT departments no longer need to worry about maintaining the back-end infrastructure and extensive data centers. With everything stored on the cloud, businesses can reduce the number of servers they run, and they do not need to worry about power outages or security attacks. Office 365 comes with a 99.9 percent uptime guarantee, taking the pressure off of IT.

Office 365

Since August 1988, when Bill Gates first announced Microsoft Office, which brought together Word, Excel and PowerPoint, the suite of applications has become synonymous with business. More than 1 billion people (15 percent of the world population) use Microsoft Office.

In 2011, Microsoft made the popular Office tools even more indispensable with the launch of Office 365. The package of applications and services is cloud-based, so users can access them from any device in any location. The Office suite is now available not only for PCs, but on devices running other operating systems, such as OS X and iOS, as well as Google Android.

In addition to the traditional Office applications, Office 365 includes Exchange Online email host, SharePoint collaboration and document-management software, Lync text and video instant messaging, OneDrive online storage, Skype for Business web conferencing and OneNote for taking notes on the go.

The benefits of Office 365 extend as much to IT administrators as they do to users. Not only does Office 365 have easy-to-use management controls, but Microsoft assumes the burden of keeping systems running. IT departments no longer need to worry about maintaining the back-end infrastructure and extensive data centers.

Rather than pay separately for each of the tools within Office 365 or per device, businesses pay a per-user subscription charge. This payment structure means they do not need to purchase additional software licenses for employees who use multiple devices. Users can access all the tools they need from any computer, smartphone or tablet.

THE CURE-ALL

Moderna Therapeutics, a biotech company working to develop medicines to fight diseased tissue, has to move fast. As it works toward its goal, the company has partnered and collaborated with other drug makers and has grown its own business fourfold.

Moderna's scientists need software that can keep pace with their fast-moving, highly regulated industry. That pace is why Moderna chose to deploy Microsoft Office 365. The suite of applications lets the company scale quickly and easily and allows its employees to create and collaborate on their research. Office 365 also provides the company with the privacy and data security it needs without sacrificing its ability to collaborate globally.

The company uses Microsoft Office apps such as Excel for simulation and modeling. Office 365 ProPlus and OneDrive let users access files remotely. With Microsoft Office Online, they can store files in the cloud and edit them simultaneously. And they use SharePoint Online integrated with Azure to enable multifactor authentication.

The cloud-based subscription model gives organizations flexibility to add or decrease licenses as needed. That can be particularly valuable in certain segments, such as retail, in which staff swells during the holiday season. Since they no longer have to purchase software and the hardware to run it on, enterprises can count Office 365 as an operating expense and save their capital budgets for other expenses.

That payment structure has translated into big savings for businesses. A Forrester study found that Office 365 delivers a 321 percent return on investment within two months for the average midsize entity. Those cost savings came from productivity gains, fewer hardware and software costs, web conferencing savings, reduced IT support and more.

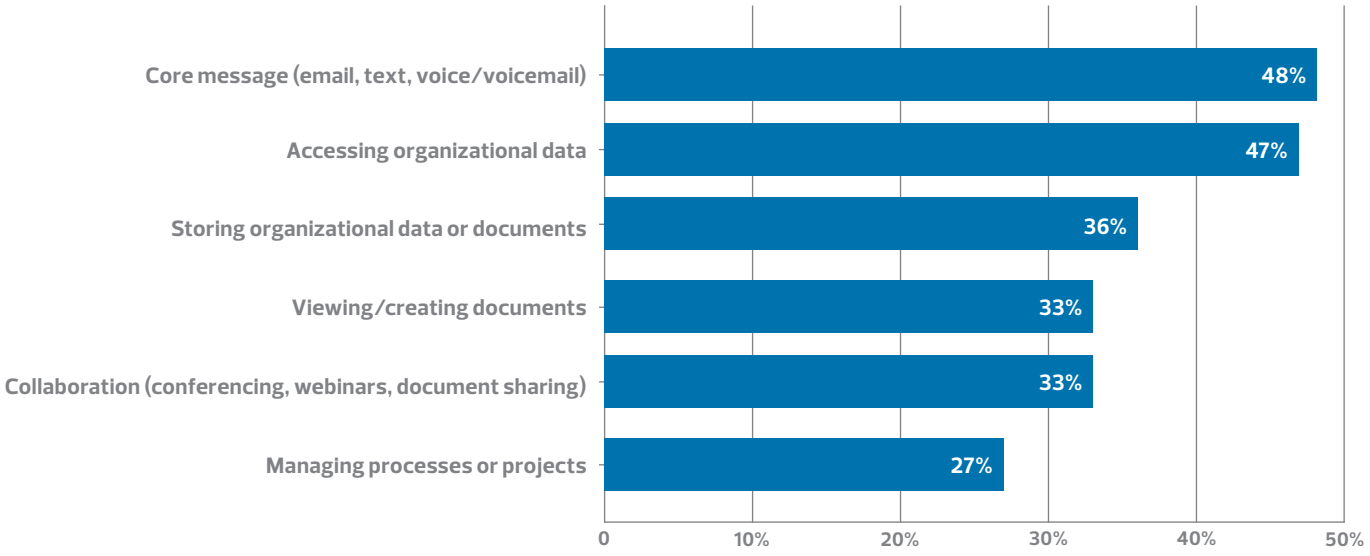
System Center

Many IT departments are already using Microsoft's System Center 2012 R2 Configuration Manager (SCCM) as a day-to-day asset management tool for servers, desktops and notebooks. Not only are administrators familiar with this advanced tool, but it easily integrates with Intune, which can extend its management capability to include mobile infrastructure. Once Intune and SCCM are integrated, administrators can manage their on-premises infrastructure and mobile devices through a single console. It is akin to adding a mobility workspace within SCCM.

Integrating Intune with SCCM helps organizations address a variety of software challenges, including:

- **Monitoring:** Administrators can use SCCM and Intune to keep tabs on all the computers, servers and mobile devices in an organization. This perspective provides a bird's-eye view of the health of the entire infrastructure right in the management console. If there is a problem with a device, SCCM alerts administrators and provides remediation capabilities.
- **Provisioning:** SCCM and Intune let administrators easily deliver applications based on corporate identity, so that users can access the applications they need on all of the devices they use to do their jobs. Users can also install applications on their own through a secure, managed company portal. When SCCM and Intune are integrated, they also simplify the software update process by identifying devices that are not up to date and installing updates as needed.
- **Configuration:** SCCM and Intune bring together all of the client management capabilities in an organization through SCCM's Configuration Manager Admin Console. It allows administrators to create settings for passwords, security, roaming, encryption and wireless communication.
- **Protection:** System Center Endpoint Protection deploys software updates and anti-malware protection. It also allows IT administrators to wipe devices if they are lost or stolen or if a user leaves the organization.

WHICH FUNCTIONS DOES YOUR ORGANIZATION PLAN TO SUPPORT VIA THE PERSONAL MOBILE DEVICES EMPLOYEES USE FOR WORK?



SOURCE: CDW's Mobility at Work Report, September 2013

Intune

While mobility brings efficiency, flexibility and new capabilities to the workplace, it can also bring headaches for the IT staff. Three-quarters of U.S. IT professionals believe their mobile endpoints had been the target of malware in 2014, according to a January 2015 report by the Ponemon Institute.

A major problem with mobility is the number of devices IT departments must manage. Previously, most users had one computer. Today, users may have notebooks and desktops as well as tablets and smartphones. These devices may all run on different platforms and operating systems. Some are enterprise devices, others are personal devices, and they are often all used for both personal and work functions.

The portability of mobile devices is another obstacle. Because mobile devices are small enough to fit into a purse or pocket, users bring them everywhere. As a result, they are easily lost or stolen. A person is 15 times more likely to lose a mobile phone than a notebook computer.

Portability also means employees will frequently try to connect mobile devices to whatever network they can find while on the go, including unsecured networks. This raises the likelihood that sensitive data can be seen by people outside the organization.

The risks add up. Unfortunately, many entities have been forced to put a price tag on those risks. Mobile security issues cost four in 10 businesses more than $250,000 last year, according to an October 2014 TechRadar report, and 80 percent of those surveyed believed that 2015 would be even worse when it comes to mobile security.

To regain control of their network and infrastructure, many organizations deploy mobile device management solutions. Part of Microsoft's Enterprise Mobility Suite (EMS), Intune is a cloud-based tool that allows IT administrators to manage devices and applications so users can access company data and applications from any device in any location without compromising corporate networks or data. Although Intune offers an array of advantages, its primary benefits include:

- **Device choice:** With Intune managing mobile devices connected to the network, users can employ either enterprise or personal devices. They simply register the device with Intune, and the IT staff can manage the corporate applications and data on it.
- **Data protection:** In addition to managing devices, Intune helps IT departments to control access to data. With this solution, they can assign and enforce user permissions, limit which applications and users can access specific data, remotely reset passwords, encrypt data or even wipe a phone.

  For instance, IT can restrict users from saving data to personal drives or emailing it. They can adjust settings so that data can be copied only from, for instance, Microsoft Word to Excel or vice versa. They can even disable the cut, copy, paste and save tools in certain applications.

80%

The percentage of Fortune 500 businesses that are on the Microsoft cloud

SOURCE: Microsoft, "Microsoft by the Numbers," February 2015

IT can also deploy mobile security settings to all devices or create profiles for users accessing resources such as email or virtual private networks. Administrators can require passwords and dictate criteria, restrict how cameras can be used on devices and set up conditional access policies within Intune. For instance, an employee may be able to access email, but only if the device meets certain security requirements.

If a device is lost or stolen, an administrator can use Intune to remotely reset the password, lock the device, encrypt the data or wipe data and applications from the device.

- **Enterprise integration:** Intune integrates easily with other EMS components, which makes it easy to deliver a consistent experience for users and administrators. This integration means that users can often have the same account information across devices and applications, and administrators can manage both mobile and on-premises infrastructures from a single console. Integration is made even easier because most IT professionals are already familiar and comfortable with Microsoft tools.
- **Cloud delivery:** Since Intune is cloud-based, organizations do not need to worry about replacing, housing and maintaining a physical infrastructure. They do not have to deal with server hardware, storage or other back-end infrastructure. Microsoft configures everything on the back end. As a result, deployment can take days rather than months — at a far lower cost.

Enterprise Mobility Suite

A quarter-century ago, when personal computers started playing a critical role in the workplace, Microsoft brought together its most popular applications — Word, Excel and PowerPoint — into a suite of tools called Office. Last year, at the peak of the mobility revolution, the company made a similar move with its mobile products.

Microsoft's EMS is designed to manage mobility enterprisewide. All of the management tools offered by Microsoft are designed to boost efficiency and security. When brought together, they are more powerful and cost-effective. EMS gives enterprises an integrated, cloud-based package of tools to keep identities, devices, apps and data safe in the cloud.

The suite consists of three main elements:

1. Cloud-based mobile application and mobile device management provided by integrating Intune into SCCM
2. Identity and access management through Azure Active Directory Premium, which allows single sign-on and uniform authentication across all devices and applications (essentially, taking the user accounts from Active Directory which IT uses for on-premises machines and applying them to mobile devices that connect to the cloud)
3. Data protection through Azure Rights Management Services, which protects data on a mobile device.

With EMS, IT staff can manage:

- **Users with a consistent identity:** IT departments have long struggled to keep corporate data and infrastructures secure without preventing employees from accessing the devices, systems and content they need to do their jobs. EMS extends the Azure Active Directory identity management services that many organizations already use in their corporate data center to the devices and applications that employees access via the cloud. Whether a user is sitting at a desktop in the office or working on a tablet at a construction site, he or she uses the same password to log on to the device and access Office 365, as well as thousands of other cloud-based applications.

  Access-control tools in EMS also keep devices and data secure. For instance, Azure Active Directory enables multifactor authentication, which offers an additional layer of security to

FLEET MANAGEMENT

Empire Today, a national flooring company, has deployed Intune to manage more than 1,200 tablets used by sales contractors. The company uses mobile devices to standardize its sales process and improve data capture as sales staffers provide quotes to customers. The company's tablets run Windows 8.1 as well as a custom app that streamlines service for mobile workers.

The company deployed Intune to centralize management of its fleet of tablets. Empire also uses the Configuration Manager to distribute its custom sales app, known as PrecisionQuote, as well as updates to the app.

Intune is helping Empire to achieve new levels of customer service. Integrating Intune and Configuration Manager allows IT administrators to remotely wipe tablets, inventory hardware and software, and automatically install apps and upgrades. The tablets provide sales staff with access to real-time product data, helping them to generate more digital quotes and orders.

34%

The percentage by which enterprise apps increase worker productivity

SOURCE: Fliplet, "10 Amazing Enterprise Mobility Facts," October 2014

prevent unauthorized users from gaining access if a password is compromised. The directory also accumulates data for reporting and learns security patterns. For example, it would flag suspicious behavior if a user were to log in from Los Angeles one minute, then Malaysia an hour later.

Azure Active Directory lets users reset passwords after answering a few questions online. Since password resets are one of the top services performed by call centers, making it a self-service task can result in big cost and time savings for IT departments.

- **PCs and mobile devices:** Intune integrates with SCCM to extend its reach to cloud-based devices. Using Intune and SCCM, IT departments can configure and manage Windows, iOS and Android devices from one console. If a device is lost or stolen or if an employee leaves the company, an administrator can remotely lock the device, reset the password or wipe data from it. If it is a personal device used for business, the administrator can do a selective wipe and erase only the corporate data and apps from the device.
- **Mobile, desktop and cloud-hosted applications:** Not only does EMS manage Microsoft applications on the desktop, it also manages 2,500 cloud and mobile apps. Users can access managed apps without remembering multiple user names and passwords. Intune can push apps from the Google Play, iTunes and Microsoft stores to user devices, or users can download them from a self-service company portal.
- **File-level data protection:** The Azure Rights Management System (RMS) manages and keeps the data itself secure. RMS lets administrators set policies that dictate who has permission to access data — within and outside of the company — and it enables encryption of files both at rest and in transit.

The Enterprise Mobility Suite combines in a single license all the tools necessary to manage an on-premises and mobile infrastructure. The tools were designed to work together efficiently, are easy to implement and help to streamline updates across the organization.

EMS is also more cost-effective than purchasing piecemeal solutions. It operates on a per-user basis (rather than by number of devices or applications). Therefore, it can cut the cost of mobility management in half. Organizations can deploy multiple devices per user or adopt bring-your-own-device policies and take advantage of Software as a Service applications without worrying about growing costs.

EMS offers a simple, cloud-based alternative to incorporating stand-alone tools into an existing infrastructure. The services within EMS — Azure Active Directory, Intune and Azure RMS — are delivered via the cloud. When integrated with other Microsoft products, they give businesses a complete, central solution for managing and protecting all of their IT resources.

To learn more about Enterprise Mobility Suite, check out Microsoft's EMS data sheet.

The Importance of Effective Integration

While users and business leaders recognize the value of mobile technology, IT departments have concerns about the challenges and risks posed by a mobile workforce. Among them is the lack of a comprehensive system with which to manage devices. In fact, a December 2014 Forrester study reported that only 14 percent of IT decision-makers say their companies have a fully robust and integrated ecosystem.

Many IT departments are still managing complex legacy systems from their pre-mobile days. The last thing they want to do is to add a hodgepodge of tools. Just as each tool is an important part of a mobile architecture, it is equally important that those tools work well together. Without that integration, IT departments will, at best, deal with chaos; at worse, they will leave their infrastructure vulnerable to malicious attacks.

As businesses look to integrate their mobile infrastructure, it is important to keep the following best practices in mind:

- **Make application security a top priority:** Intune can help with both device and application management, ensuring that the devices and the applications used on those devices are properly and efficiently deployed, managed and protected.
- **Help users help themselves:** Users are not new to the world of mobile devices. The large majority have smartphones or tablets that they use on the job. Self-service functions, such as allowing users to reset their passwords or download apps from a company store, can save the IT department valuable time.
- **Manage mobile updates:** Because of mobile devices' vulnerability to security risks, it is more critical than ever for IT to keep up with updates. With Microsoft Enterprise Mobility Suite, all of the Microsoft tools are managed together and are automatically updated.
- **Enforce secure authentication:** EMS enables users to have a single sign-on across devices and apps, but it also has controls in place to protect accounts. With multifactor authentication, for instance, users can be prompted for an additional way to confirm their identity.

- **Test mobile systems with limited rollouts:** Rather than conduct a massive implementation across the company, it makes sense to test new mobile systems with pilot groups. Roll out the technology to larger groups after working out the kinks.

CDW: A Mobility Partner That Gets IT

More than a quarter million businesses turn to CDW for their technology needs. Dedicated teams of CDW account managers, engineers, field technicians and solution architects work day to day with customers to build new systems and transition from legacy platforms. If customers have questions along the way, they can call and speak with one of the top experts in that field.

Because it purchases in volume, CDW is also competitive when it comes to price. CDW representatives can help customers get the same products for less. In addition, we have a long, close collaborative relationship with Microsoft, which can translate into cost savings and greater access to Microsoft professionals for customers.

CDW can help customers plan, design, implement and integrate Microsoft Enterprise Mobility Suite with Office 365. While the products within the suite are designed to be easily integrated, there are nuances that experienced integrators know how to draw out for maximum benefit.

By working with an experienced partner to integrate the products in the suite, organizations can get a far more valuable solution than if they had pieced products together on their own. CDW gets IT, it gets Microsoft and it gets mobility. And it can help businesses get there too.

To learn more about CDW's mobility products and services, call your account manager, dial 800.800.4239 or visit CDW.com/mobility.

Microsoft

Microsoft® offers a substantial lineup of mobility products to meet your organization's needs — including the Surface™ Pro 3 and the Surface 3. Fold back the Surface keyboard, and you have the perfect hand-held, touch-screen tablet. The Surface USB port lets you plug in a wireless mouse or share files with a thumb drive. Its video-out port allows you to connect to an external monitor so you can work like you would on a desktop. Take your pick of thousands of apps in the Windows app store. While providing great productivity and ease of use for your organization, Microsoft products offer easy, secure integration into your environment.

CDW.com/microsoft