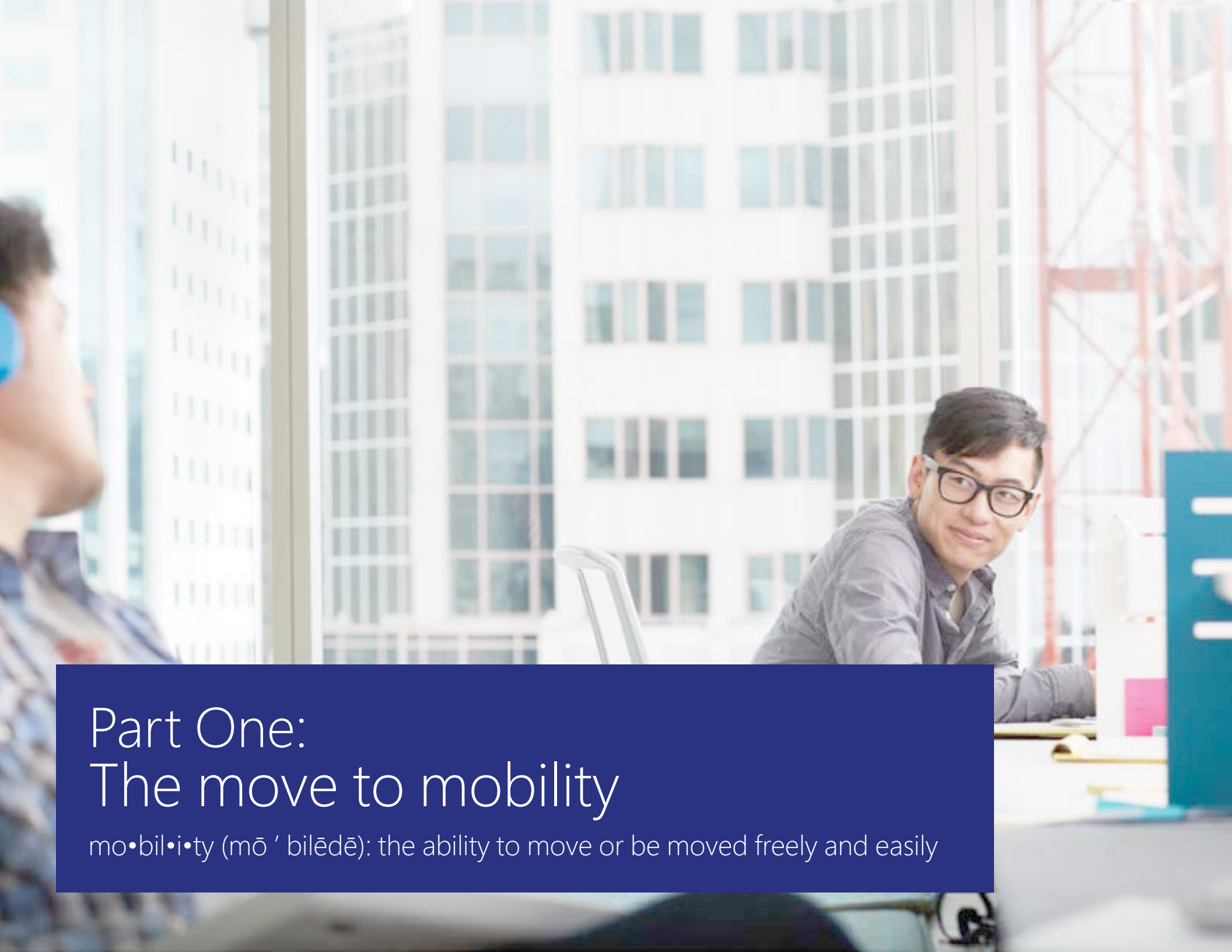
Controlling the uncontrollable

Why you need to enable, protect, and manage mobile productivity end to end

Microsoft

Table of Contents



Part One:
The move to mobility

mo•bil•i•ty (mō ′ bilēdē): the ability to move or be moved freely and easily

Part One:

The move to mobility

Mobile devices are everywhere in the enterprise today, with many more devices on the way as companies embrace the mobile work world. Users expect to be productive across a variety of device types with constant access to the applications they need. Terms like bring your own device (BYOD) and enterprise mobility management (EMM) aren't just buzzwords or passing fads. They're a key strategy of most IT departments to support the consumerization of IT and the empowerment of users, however those users want to work. Every industry is being transformed by the trend toward cloud and mobility. The catch-phrase "work from anywhere on any device," a pipe dream 25 years ago, is now the standard for most enterprises in a mobile-first, cloud-first world.

Consider these facts

- The number of mobile devices worldwide is the billions
- 29% of workers use three or more devices, work from many locations, and use many apps
- 80% of workers admit they use nonapproved apps at work
- 67% of workers who use a smartphone at work chose it themselves
- 70% of workers who use a tablet for work chose it themselves

Part Two:
The four elements of enterprise

Part Two:

The four elements of enterprise

To address enterprise mobility challenges, it helps to understand the four elements of an enterprise mobility strategy:

1. Users
2. Devices
3. Apps
4. Data

1: Users

The most important elements of an EMM solution are the users or employees. Without them, the costs and IT infrastructure to enable enterprise mobility are meaningless. Users expect to be able to work in any location and have access to all their work resources as they work. To enable that, an EMM solution must make it as easy as possible for IT to manage user accounts and for employees to access company resources. If an IT administrator finds user identity hard to manage, or if an employee must take overly complicated steps to gain access to devices or resources, an EMM solution is not worth whatever you're paying for it. IT needs effective user identity management tools.

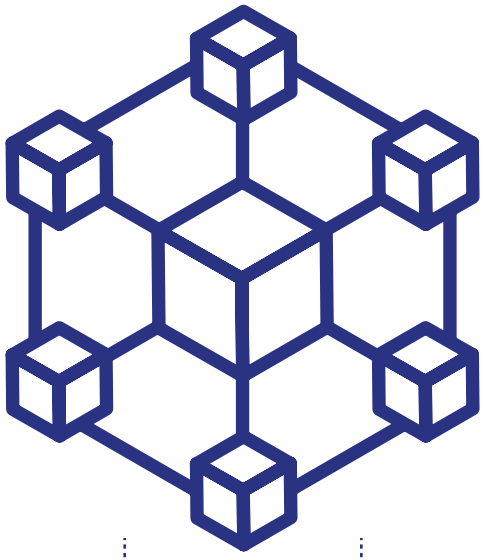
One way to think about users is by defining typical user personas such as these:

- **Executives.** They expect the company to buy them whatever device they want to use as their primary device. Executives aren't likely to be BYOD users.
- **Mobile workers.** They encompass a large group of employees that is accustomed to using multiple devices.
- **Technical field workers.** They require a robust device to perform their work. Usually they primarily use line of business (LOB) applications and email and enter data into customer relationship management tools.
- **Desk-bound information workers.** They use a variety of devices and enroll in the BYOD program. From taking notes in meetings on their own companion devices to potentially wanting to use their own machines while in the workplace, these users are likely to drive most of the BYOD adoptions in the company.
- **Remote information workers.** They look to optimize their workspace, blending personal priorities with company priorities. They might be good candidates for the BYOD program.

2: Devices

The rapid pace of technological advancement has changed the modern workplace from one of stationary workstations and company-issued devices to one that includes an ever-expanding array of mobile computers and Internet-connected devices. Using their personal mobile devices—such as smartphones, tablets, and laptops—employees are increasingly mixing their personal lives with their work responsibilities. The explosion of devices is eroding the traditional standards-based approach to corporate IT hardware procurement. This change is driving the BYOD trend across all markets and industries. IT departments thus are tasked with managing a collection of different types of mobile devices, operating systems, and vendor-specific requirements. IT needs effective device management tools.

In the enterprise, mobile devices are hard to detect, let alone control—a huge problem. The number of unmanaged, data-leaking, potential-perimeter-intrusion devices in enterprises today is staggering. How did we get here? A major culprit is the common practice of approaching the future of IT with the same tactics used in the past. Today's end users vigorously resist having their devices managed because the productivity apps (or emulated apps) are awful, the devices get slower, and the organizations that manage these devices never really grasped how to best empower their workforce.



Here are two common scenarios where devices often put an enterprise at risk:

- **Loss or theft of mobile devices.** The responsibility for the loss or theft of data on an employee-owned device is a challenge. Deleting an employee's data from a personal device is often impractical and can have legal implications. What's more, some employees share their personal devices with family members. An employee sharing a BYOD device with his or her spouse invites the potential for serious issues, such as corporate data loss or security breaches. IT needs the right tools to prevent these problems.

- **Sale of personal mobile devices.** Another risk scenario that IT must address is when employees sell or recycle their own devices after those devices have been used to access company data. A common strategy is to require remote wiping of the device's data as a condition of access to corporate data. But IT requires the tools to do that.

3: Apps

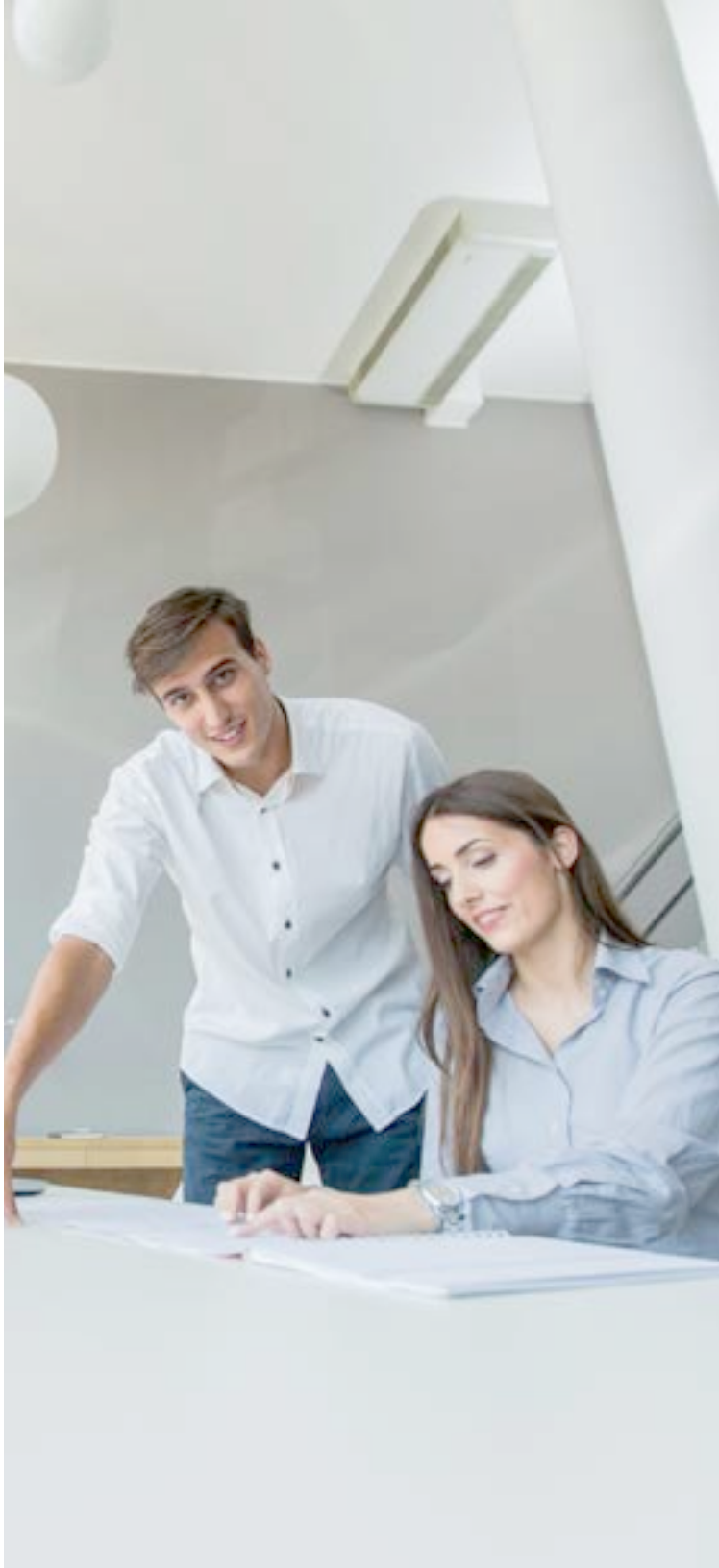
Apps are the centerpiece of most business requirements and the portal for information access for most modern organizations. Though managing different device types creates new administration challenges, managing a mixture of commercial and customized LOB apps can be equally challenging. And deploying and managing applications across platforms continues to be difficult. Employees need access to all their productivity tools from all their devices, including email, data storage services, and role-specific tools. These services can be either locally hosted in on-premises networks or hosted in the cloud.

Proliferation of productivity apps in the cloud is causing headaches for IT in some enterprises. The real problem is that the knockoff productivity apps (the ones mimicking the Microsoft Office apps) provided by the various EMM vendors are not great. These knockoff apps don't do enough to protect corporate data, and the user experience doesn't empower the end users.

Different apps have different installation requirements, can require individual adjustments to function properly on different devices, and often have varying levels of risk associated with keeping information secure. Misjudging or improperly managing any of these areas can lead to exposing sensitive company data or employee personal information. IT departments must take care to fully understand which apps will be supported and how they will be managed to help protect company data. IT needs effective mobile application management tools.

Apps are the main gateway to information for most users, so as you develop a strategy for apps, you must:

- **Define** which apps will be available for the users to consume using their devices
- **Validate** if those apps need any type of adjustment to correctly run on different platforms
- **Assess** possible threats on each app that will be available for mobile users and verify if there is any flaw that can lead to a security risk
- **Mitigate** potential flaws by fixing the root cause of the problem or adding countermeasures that can reduce the risk
- **Verify** how these apps will be available for users' consumption from those different devices
- **Enumerate** the options that are feasible for your business to make those apps available (for example, deployment via Web portal, access via remote app, access via VPN, and so on)



4: Data

Working from a mobile device from any location really means accessing data from anywhere. Users need to be productive while maintaining compliance and reducing risk. Operating hand-in-hand with identity management, apps, and the architecture of mobile devices, data must be consumed securely and easily for users to be productive and to keep them from finding alternative access routes to information. Understanding how data is stored on devices and how data is protected in transit is critical when planning and configuring enterprise mobility management features and policies.

Company data must be protected at all stages: while data is in the cloud, while data is at the company's datacenter, while data in the user's device, and while data is in transit between any (and all) of the aforementioned locations. What's more, company data must be isolated and protected from a user's personal data while also securing a user's privacy. And IT must also maintain regulatory compliance.

Depending on business needs and user requirements, your organization might require multiple layers of data protection, ways to classify information according to sensitivity, methods for data encryption, and integrated ways to manage access control. Different enterprise mobility management solutions offer varying levels of control for each of these areas and offer different levels of reporting and monitoring in the case of breaches. IT needs effective data management tools.

The key to a successful EMM solution is to let users consume company resources without compromising data. An EMM solution should include:

- **Security envelopes** to protect data
- **Data encryption** to protect files
- **Safety policies** that control access and reporting
- **Multifactor authentication (MFA)** or a similar level of extra authentication
- **Business-driven** policies for data protection
- **Classification of data** by sensitivity and business impact
- **Access control** to data based on identity and role

Part Three:
If your organization uses Microsoft Office, its ready for mobility

Part Three:

If your organization uses Microsoft Office, its ready for mobility

Just about every one of our conversations with customers eventually comes back to Microsoft Office and the Office mobile apps. Consider this question we often ask: How much of your organization's day-to-day work relies on Microsoft Office? Your accounting and financial department probably has Microsoft Excel open all day everyday—and your IT department probably has it open to keep track of who has been assigned each IP address! Your executives are regularly reviewing and presenting with Microsoft PowerPoint. And, in most cases, every person in your org uses Microsoft Outlook. In meetings with customers, we often ask them what percentage of the docs that are shared and used in their organization are Office docs. The answer is consistently between 75% and 95%.

If any of this sounds familiar, then your organization is already prepared to become more mobile. At Microsoft, we sit in a unique position to take the infrastructure you're already using and make it more secure and more mobile right now.
This process is something that any organization can undertake, and we have worked exhaustively to make Microsoft the single best option for this exciting transition. The reason behind this confidence is simple: When it comes to enabling Microsoft Office on all the devices in your organization and managing and securing all these identities and data with an EMM solution, no company can manage and secure this better than Microsoft.

Part Four:
Many EMM vendors are struggling. Which will survive?

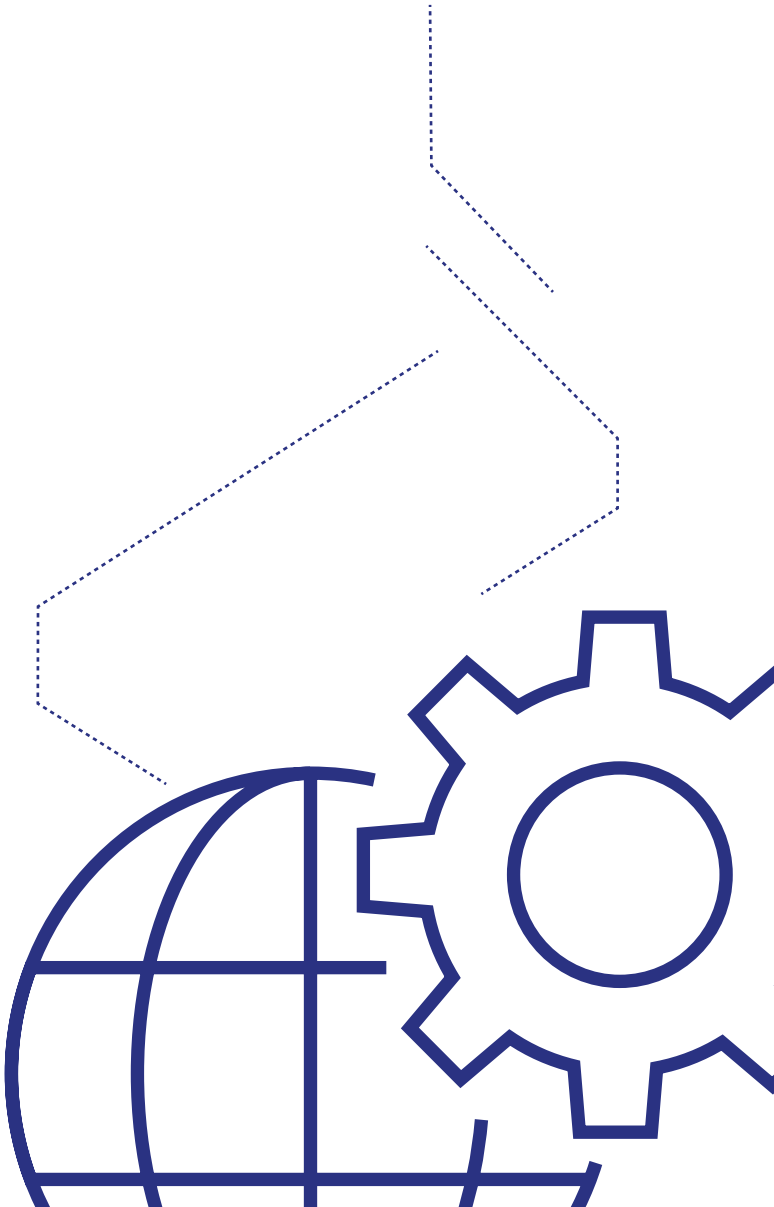
Part Four:

Many EMM vendors are struggling. Which will Survive?

Compounding all the challenges that we've outlined so far is how quickly and easily EMM vendors come and go. When you're planning your work with an EMM vendor, you must ask yourself if that vendor will exist in 12, 18, or 24 months. Depending upon your deployment plan, your vendor might not even exist by the time you're fully deployed! This means you have to ask yourself if you're going to get your ROI in two years or less. You also have to ask if your on-premises investments are going to work with the cloud-based assets you'll be incorporating. And you also have to look at whether these new solutions are really built as services from the cloud so that they can scale. You need to ask the type of productive questions that will put your organization on a proactive footing: Identify the challenges you're facing, and then demand your vendor provide integrated solutions.

Some of the questions you should ask include:

- What productivity apps do you currently use (or plan to use)?
- Do you plan to use inbox or app-based email?
- What types of devices do you need and plan to support?
- Who's going to own the devices you manage?
- Will personal and corporate devices be managed the same way?



A lot of vendors can't answer these questions. A lot of others will hedge. But your organization deserves concrete answers. To find out more, watch this video clip:

Problems with EMM vendors

To put mobility and management in perspective, you can do some simple math to see that only a small percentage of the world's devices are being managed today—even when you include the work being done by every EMM vendor:

- The number of devices around the world reaches well into the billions.
- The number of EMM licenses is slightly over 100 million.
- The number of activated licenses is (optimistically) in the tens of millions.

There's no shortage of narrow-point solutions that can provide bits and pieces of the overarching solution you need—but modern IT departments face enough day-to-day challenges without having to constantly fine-tune and integrate a bunch of different products. To show you what this looks like in real life, check out this quick segment from a new Enterprise Mobility Suite (EMS) training video:

The Best EMS Overview Available

Part Five:
Microsoft Enterprise Mobility Suite is the mobility solution you're looking for

Part Five:

Microsoft Enterprise Mobility Suite is the mobility solution you're looking for

Fortunately, Microsoft has a complete solution to help make your organization better equipped to go mobile, stay mobile, and protect your data. Microsoft EMS is Microsoft's comprehensive cloud solution for your BYOD and EMM challenges. Microsoft EMS has grown at an unbelievable rate because it's the solution companies like yours need. Microsoft EMS consists of three elements:

Microsoft Azure Active Directory Premium for hybrid identity and access management

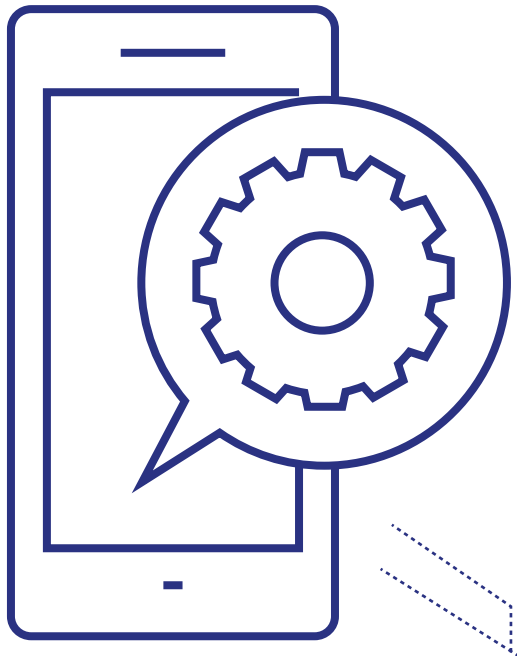
Microsoft Azure AD Premium delivers robust identity and access management from the cloud, in sync with your existing on-premises deployments:

- Cloud-based self-service password reset for your employees
- Group Management, including user self-service management of groups
- Group-based provisioning and access management for hundreds of software as a service (SaaS) applications
- Machine-learning-driven security reports to show login anomalies and other threats
- Rich and robust synchronization of user identities from on-premises directories, including write back of changes
- Reduce risk and support compliance requirements with comprehensive MFA options

Microsoft Intune for mobile device and application management

Microsoft Intune provides mobile device management, mobile application management, and PC management capabilities from the cloud:

- Deliver mobile device and application management across popular platforms: Windows, Windows Phone, iOS, and Android
- Maximize productivity with Intune-managed Office mobile apps, and extend mobile application management to line-of-business apps with the Intune app wrapper
- Provide access to corporate resources on devices based upon enrollment and compliance policies
- Simplify administration via a single management console in the cloud with Intune or on-premises through integration with System Center 2012 Configuration Manager



Microsoft Azure Rights Management for information protection

Microsoft Azure AD Premium and Azure Rights Management can help protect your corporate assets:

- Deliver information protection in the cloud or in a hybrid model with your existing on-premises infrastructure
- Integrate information protection into your native applications with an easy-to-use software development kit

Part Six:
Why Microsoft EMS is the best EMM solution for your organization

Part Six:

Why Microsoft EMS is the best EMM solution for your organization

Architecture matters. That's why our enterprise mobility solution is designed to run in the cloud and work with your current on-premises infrastructure. Our cloud-first approach to managing a mobile enterprise is the fastest, most cost-effective way to meet new business challenges and accommodate new devices, new apps, and new hires—without worrying about scale, maintenance, or updates.

Here's why you'll love Microsoft EMS:

- It protects Office better. It's the only solution designed to protect your Microsoft Office email, files, and apps
- It saves you money. It costs up to 50% less than the cost of buying standalone solutions from other vendors
- It just works. It's simple to set up, always up to date, and connects to your existing on-premises resources
- It's integrated. One identity platform protects them all—users, devices, apps, and data
- It's comprehensive. It includes data protection support for iOS, Android, Windows, Windows Phone, and over 2,500 popular SaaS apps

Users

Microsoft EMS provides single sign-on to thousands of popular, pre-integrated SaaS apps such as Salesforce, Concur, and Office 365. Single sign-on and directory synchronization extend your directory services to the cloud and provide your users with a high-fidelity authentication experience.

- MFA offers better security for your corporate resources by requiring additional verification from users beyond their usernames and passwords
- Users access both cloud and on-premises resources with their existing on-premises credentials
- Self-service management features allow users to reset passwords and lock or wipe their mobile devices

Devices

With Microsoft EMS, you can connect your on-premises resources, such as Microsoft Exchange and SharePoint servers, to leverage the power of cloud services.

- Tight integration of Intune and System Center Configuration Manager helps you virtually manage devices and PCs from a single management console
- Includes conditional email access to your mailboxes hosted on Exchange Server or Exchange Online, as well as access to SharePoint Online
- Mobile Application Management separates your corporate apps and data from users' personal apps and data and enforces security policies on corporate resources

Apps

With Microsoft EMS, you can stream applications from on-premises or the cloud to keep users productive anywhere, on any device, and your company data more secure.

- Session-based desktops and Azure RemoteApp offer a scalable platform that delivers your corporate applications simply and cost-effectively
- Users install Microsoft Remote Desktop clients and run personal virtual desktops and apps on their laptops, tablets, or phones and stay productive on the go
- Pooled virtual desktops on Azure scale up or down to meet dynamic business needs

Data

With Microsoft EMS, you can deploy and configure access to corporate resources across your on-premises environment and cloud applications while helping to protect corporate data. You remain in control of your data, even when it's shared with others.

- Encryption policy at the file level follows documents inside and outside your organization
- Collaborate more securely by protecting any file type on any device platform using Azure Rights Management
- Safely share files in email or use your favorite cloud storage service, such as Microsoft OneDrive

Part Seven:
Further Resources

Part Seven:

Further Resources

Microsoft has a wealth of resources to help your move to mobility.

- **Want to read more?** Read the posts in our EMS series
- **Have a few minutes?** Check out the Enterprise Mobility Pit Stop tutorials
- **Have a few hours? Deep dive with the** Enterprise Mobility Core Skills courses
- **Need documentation?** Microsoft Intune TechNet Library
- **Ready to get hands on? Sign up for an** Enterprise Mobility Suite trial
- **Ready to convince your boss? Download the** IDC Technology Spotlight: Securing Productivity in the Borderless Enterprise