Microsoft

Enterprise Mobility Suite

Managing BYOD and Company-Owned Devices

Yuri Diogenes
Jeff Gilbert

Foreword by Brad Anderson
Microsoft Corporate VP, Enterprise Client & Mobility

Microsoft

Enterprise Mobility Suite: Managing BYOD and Company-Owned Devices

Yuri Diogenes
Jeff Gilbert

PUBLISHED BY
Microsoft Press
A Division of Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052-6399

Library of Congress Control Number: 2014955635
ISBN: 978-0-7356-9840-6

Printed and bound in the United States of America.

First Printing

Microsoft Press books are available through booksellers and distributors worldwide. If you need support related to this book, email Microsoft Press Book Support at mspinput@microsoft.com. Please tell us what you think of this book at http://www.microsoft.com/learning/booksurvey.

Acquisitions Editor: Karen Szall
Developmental Editor: Karen Szall
Editorial Production: Box Twelve Communications
Technical Reviewer: Randall Galloway; Technical Review services provided by Content Master, a member of CM Group, Ltd.
Copyeditor: Box Twelve Communications
Indexer Box Twelve Communications
Cover: Twist Creative • Seattle

Contents at a glance

This page intentionally left blank

Contents

What do you think of this book? We want to hear from you!

Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

microsoft.com/learning/booksurvey

What do you think of this book? We want to hear from you!

Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

microsoft.com/learning/booksurvey

This page intentionally left blank

Foreword

Of all the books you'll read about the Enterprise Mobility Suite, this one is probably the first. In my opinion, it is also the most comprehensive to date.

Enterprise Mobility Management—the thing that EMS so brilliantly supports and empowers—is one of today's defining trends, and it is the core area of focus for some of the most brilliant software architects and developers in the tech industry. The reason is obvious: No other technological development will have a greater impact on the way we live and work than our current device ubiquity.

From an IT perspective, the number of devices your users want to use, the volume of data they access, and protecting those corporate assets (and the end users themselves) are just a handful of the incredibly serious issues you must face every day. This reality is what makes EMS so exciting; it represents the intersection of great software architects with the IT teams working on the front lines of organizations all over the world. With this cloud-based technology, and by leveraging things like Machine Learning from the cloud, the feedback loop is faster than ever. Now you can enable your users in ways you never have been able to in the past.

In this book you'll see—in practical terms and examples—how to make these devices and the people using them dramatically more productive, more connected, and more secure. From the back end of your infrastructure (Microsoft Intune, Azure Active Directory Premium, Azure AD RMS) to the apps your end users interact with every day (Office 365), EMS is an incredibly sophisticated set of tools that dramatically simplify many previously intractable technical challenges.

The Enterprise Mobility Suite is where I believe a cloud-first, mobile-first perspective really takes shape. The speed of business, the constant movement of workers and data, and the need to keep innovating are all delivered with the entirely service-based solutions offered by the EMS. It's powerful, reliable, and offers you the cross-platform functionality that's required to help you successfully and optimistically bridge your organization's past and future.

Jeff and Yuri have spent an exhaustive amount of time with every corner of the Enterprise Mobility Suite, and this book will prepare you to use it to solve the unique challenges your organization is facing today—and to plan ahead for your organization's long-term success.

Brad

Brad Anderson, Microsoft Corporate VP, Enterprise Client & Mobility, @InTheCloudMSFT

This page intentionally left blank

Introduction

This book provides you with an introduction to the Enterprise Mobility Suite (EMS). In it, you are put in the driver's seat through scenario-based content covering each of the independent technologies that make up EMS: Microsoft Azure AD Premium, Azure Rights Management Services (RMS), and Microsoft Intune. Throughout the chapters, we guide you through the process of implementing EMS to support Mobile Device Management (MDM) of both company-owned devices and personally-owned devices in your enterprise environment.

The scenarios described in this book are truly end-to-end. Starting with enabling hybrid identity, you will quickly learn how to secure corporate data access, protect your employees' personal information, manage iOS, Android, and Windows devices, and, finally, how to monitor and perform basic troubleshooting of all EMS components.

The target audience for this book is comprised of enterprise IT Pros who are either charged with implementing EMS for their organizations or just want to learn more about the technologies that are included in EMS. While it is not possible to cover every aspect and nuance of the technologies included in EMS in a single book, we have attempted to include the content we believe will provide you with the solid foundation you will need as you begin your own EMS implementation journey.

Acknowledgments

The authors would like to thank Karen Szall and the entire Microsoft Press team for their support in this project, Brad Anderson for writing the foreword of this book, and all of our Microsoft colleagues who contributed by reviewing this book: Ben Hawken, Simon May, Robert Mazzoli, Sonia Wadhwa, Eddie Bowers, Keith Brintzenhofe, Marsha Shoemaker, Taylor Thomson, Ken Hoff, Gil Lapid Shafriri, Debbie Furtado, and Stacey Ellingson. We would also like to thank the Microsoft MVPs who reviewed this book: Kent Agerlund, Kenny Buntinx, Peter Daalmans, John Marcum, Torsten Meringer, Stefan Schörling, and Steve Thompson.

Yuri Diogenes I would also like to thank my wife and daughters for their endless support and understanding; my great God for giving me strength and keep guiding my path; my friend and co-author Jeff Gilbert (without you this project would not have been possible—thanks); my great friends and former co-authors

Tom Shinder and Jim Harrison (you both keep inspiring me to write); my former managers Kathy Watanabe and Jason Whitmarsh for their support when I joined the team; and last, but not least, my parents for working hard to give me an education, which is the foundation that I use every day to keep moving forward in my career.

Jeff Gilbert I would also like to thank my wife and kids for their support in always lending a sympathetic ear to my excited technical ramblings—which I'm sure sounded like a foreign language to them. This book could not have been possible without the help of Yuri Diogenes, my co-author and the one who inspired me to join him on this journey. I'd also like to thank all those whom I work with at Microsoft and my friends in the systems management IT community who have always supported me and given focus to the work I do every day.

Free ebooks from Microsoft Press

From technical overviews to in-depth information on special topics, the free ebooks from Microsoft Press cover a wide range of topics. These ebooks are available in PDF, EPUB, and Mobi for Kindle formats, ready for you to download at:

http://aka.ms/mspressfree

Check back often to see what is new!

Microsoft Virtual Academy

Build your knowledge of Microsoft technologies with free expert-led online training from Microsoft Virtual Academy (MVA). MVA offers a comprehensive library of videos, live events, and more to help you learn the latest technologies and prepare for certification exams. You'll find what you need here:

http://www.microsoftvirtualacademy.com

Errata, updates, & book support

We've made every effort to ensure the accuracy of this book and its companion content. You can access updates to this book—in the form of a list of submitted errata and their related corrections—at:

http://aka.ms/EMSdevice/errata

If you discover an error that is not already listed, please submit it to us at the same page.

If you need additional support, email Microsoft Press Book Support at *mspinput@microsoft.com*.

Please note that product support for Microsoft software and hardware is not offered through the previous addresses. For help with Microsoft software or hardware, go to *http://support.microsoft.com*.

We want to hear from you

At Microsoft Press, your satisfaction is our top priority, and your feedback our most valuable asset. Please tell us what you think of this book at:

http://aka.ms/tellpress

The survey is short, and we read every one of your comments and ideas. Thanks in advance for your input!

Stay in touch

Let's keep the conversation going! We're on Twitter: *http://twitter.com/MicrosoftPress*.

This page intentionally left blank

Chapter 1

Enabling a mobile workforce

The catchy phrase "work from anywhere" has evolved throughout the years and nowadays working from anywhere is the standard for many industries. However, as consumers started to use their own gadgets more and more to perform work-related tasks, "working anywhere and from any device" has become the new vision for many enterprises in a mobile-first, cloud-first world. This chapter explains why it is important for companies to develop an effective strategy for embracing a mobile workforce and also explains how the paradigm shift caused by the Bring Your Own Device (BYOD) trend impacts the overall strategy to securely adopt a mobile workforce.

The shift towards mobility

When companies started to understand the value of cloud computing—particularly as it related to how they could leverage its resources to be more agile and to reduce costs—they also discovered that users were already consuming cloud resources on their own devices. Cloud-based apps are intended to run on all types of portable devices. Also, cloud-based apps are usually programmed to run on several major operating systems, a strategy that drives rapid adoption from consumers. In this new era of Enterprise IT—also referred to by Gartner[1] as the "Third Era of Enterprise IT"—enterprise users not only demand agility, they demand a substantial increase in productivity.

While you might think that this concept is new, the fact is that this mobility phenomenon has been growing for at least the past seven years. A 2008 IDC study sponsored by Microsoft and performed by International Data Corporation (IDC) called Mobility Solutions in Enterprise-Sized Businesses: Quantifying the Return on Investment[2] revealed that the Return of Investment (ROI) with the use of mobility technologies pays off. So the question becomes, "What strategy should be implemented to support a mobile workforce and remain competitive in the marketplace?"

A 2014 survey[3] published by IDG Enterprise Consumerization of IT in the Enterprise (CITE) suggests that the consumerization of IT maximizes the capabilities of mobility and

---

[1] For more information about the Third Era of Enterprise IT, visit *http://www.gartner.com/newsroom/id/2649419*.

[2] You can read the entire report at *http://aka.ms/MobileROI*.

[3] You can read the entire survey at *http://www.idgenterprise.com/report/idg-enterprise-consumerization-of-it-in-the-enterprise-study-2014*.

empowers users. This survey documents several key findings. The following two key findings specifically address the trends for IT and mobile workforces; these key findings are the core foundation of this book:

- The proliferation of user-owned devices requires companies to adjust their policies and invest in Mobile Device Management (MDM) capabilities in order to maintain control over the devices while ensuring users can remain productive.
- Security is a key element to consider throughout the lifecycle of mobile devices.

These findings reinforce the fact that while CEOs are willing to enable users to be more productive by using their own mobile devices, the IT department must remain in control of those devices to ensure the company's data is protected.

The challenges of enabling enterprise mobility

To address the challenges that comes with enabling mobility in your company, you must understand the four elements of an enterprise mobility strategy (see Figure 1-1):

- Users
- Devices
- Apps
- Data

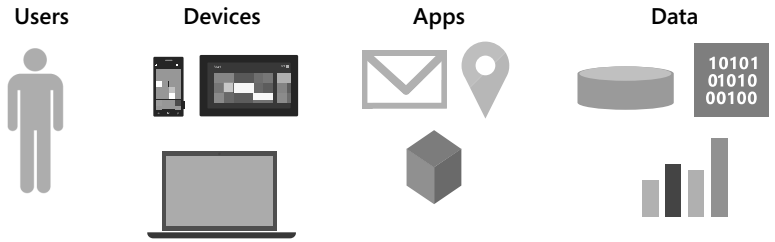

FIGURE 1-1 The four elements of an enterprise mobility strategy

When you embrace a mobile workforce, you not only must consider the user and the device he wants to use, you must consider how the apps that will be consumed will be affected by being on a mobile device. Even more importantly, you need to consider how to ensure that the company data remains secure. To effectively manage security of mobile devices, you should be sure to incorporate security into each of the four elements referenced in Figure 1-1. Focusing on each of the elements will help you to better address each challenge in a scenario-based approach. You want to ensure that your overall strategy is compliant with your business requirements while meeting the user's expectation about how she will perform at work using the device or devices of her choice.

Now that you know the elements, Figure 1-2 expands on the elements shown in Figure 1-1 and shows the three core scenarios that you will use throughout the entire book:

1. Enable users to choose their devices.
2. Unify the management of applications and devices
3. Protect corporate data.

By using this approach, you will be able to understand the challenges that must be addressed by your company before you embrace mobility.

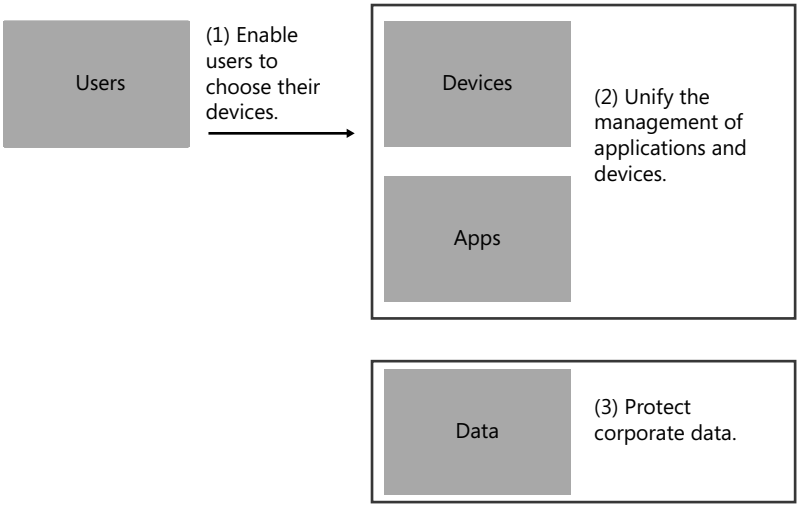

FIGURE 1-2 The three categories of challenges

As shown in Figure 1-2, the three core scenarios are bound to one or more of the elements shown in Figure 1-1. The following list explains the issues that must be addressed as part of your enterprise mobility strategy:

1. Enable users to choose their devices
   - Users want to use their own devices to access both their personal data and their work-related data/apps.
   - Users want access to these elements from anywhere.
   - While CEOs want to fulfill user requirements in order to enable users to be productive, they also want their IT department to be in control of how users access company data.
2. Unify the management of applications and devices
   - Users must have a common identity to access applications and company resources from any device and from anywhere.
   - IT must be able to manage, deploy, and maintain applications for all types of devices.

- IT must be able to manage company-owned devices as well as user-owned devices from a single location.

3. Protect corporate data
   - Corporate 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.
   - Corporate data must be isolated and protected from a user's personal data while also securing a user's privacy.
   - The IT department must be empowered to secure, classify, and protect the company's data while also maintaining regulatory compliance.

Throughout this book, these challenges will be used as examples for scenarios that explain how Enterprise Mobility Suite (EMS) can assist your company's efforts to enable a mobile workforce.

What about BYOD?

Your efforts to embrace a mobile workforce must include an effective strategy for handling the BYOD scenario. The BYOD scenario includes more than making your company "mobile ready;" it encompasses all the challenges and opportunities as well as the security risks of variations on the scenario. These variations will be explored in this chapter. Before you delve into the specific challenges involved with BYOD, think about why BYOD has become a "buzzword" and why companies should proceed cautiously when adopting BYOD.

Real World The vendor-agnostic approach to BYOD

For the past two years, I've been delivering BYOD presentations that approach the topic from the architecture perspective and explain how to build a BYOD design with a vendor-agnostic approach. My first work on this field was released in April 2014 with the BYOD Design Considerations Guide (available at *http://aka.ms/BYODCG*), which features a collection of vendor-agnostic considerations regarding BYOD and how Microsoft technologies can help your company fulfill those requirements. The presentation that I delivered at TechEd North America 2014 was based on this paper; you can watch it at *http://aka.ms/byodtena14* and learn how to use a vendor-agnostic approach when developing your BYOD strategy.

To help IT professionals to think of BYOD as a problem domain that must have design considerations and choices aligned with company requirements, constraints, and vision, I also recorded a series of interviews (*http://ala.ms/byodseris*) for TechNet Radio. These materials can help you to plan, design and build your solution to address the BYOD challenges.

Yuri Diogenes
Senior Content Developer, CSI Enterprise Mobility Team, Microsoft Corporation

A November 2013 study by Gartner suggested that 20 percent of enterprise BYOD programs will fail before 2016. The study indicates programs will fail because of mobile device management measures that are too restrictive. This study shows that companies are moving towards the adoption of BYOD, but they are restricting access and thereby not necessarily realizing BYOD's full potential. Managing security is often a delicate balance. If your security policies aren't strict enough, you'll put corporate resources at risk. If your security policies are too strict, you might create an environment that becomes a tremendous challenge for the IT department to support, thereby adversely impacting your ROI. If your BYOD security produces a higher volume of help-desk calls from frustrated users, or, worse yet, if users are unable to perform their work, you might find that your organization needs to roll back to previous technology. As a result, BYOD becomes an enemy of the company. For this reason, you must ensure that your organization defines an effective BYOD strategy before BYOD is implemented or deployed.

In October 2014, a CheckPoint survey of 700 IT professionals showed mobile security incidents caused by BYOD had cost each organization more than $250,000 US to remediate[4]. These costs are likely to increase as more organizations adopt BYOD as part of their enterprise mobility strategy—underscoring the importance of understanding the challenges of adopting BYOD.

Understanding the challenges of BYOD

Before you can understand the challenges introduced by BYOD, you must first understand your own business requirements, constraints, regulatory compliance needs, and users' needs and goals. Unfortunately, this planning phase is often completely overlooked and gaps are found when the next phase—designing the solution—is underway. The best way to mitigate risk is to be aware of how your own company operates. The assumption here is that your company already has a security policy in place. What if that security strategy does not address the security challenges that BYOD introduces to the environment? The same rationale can be applied to your current management infrastructure. What if the existing management platform does not allow users to bring their own devices or does not provide access to company resources?

The industry that your company works in also plays an important role in how BYOD should be adopted. With BYOD, the device contains both the user's personal data and the company-owned data. This results in unique challenges for each industry. For instance, in a school environment, BYOD can be very helpful; to improving user productivity; however, the challenges can be very unique, as you will see in this section of the book.

MORE INFO **Read "BYOD Devices - A Deployment Guide for Education" for a better understanding of the design considerations applicable to the education industry at *http://www.microsoft.com/en-us/download/details.aspx?id=39681*.**

[4] For more information about the core findings of this survey, visit *http://www.infosecurity-magazine.com/news/byod-security-incident-costs/*.

There are privacy elements that must be considered for both the individual and the corporation. For this reason, it is very important to involve your legal department when planning the BYOD adoption. Employees must be aware that when they enroll in the BYOD program, the devices that they use might be subject to discovery in litigation. The personal devices they use at work could be examined not only by the employer but by the other party in a lawsuit. Of course, this will vary according to country/region and state laws. As shown in Figure 1-3, the Human Resources (HR), legal, and IT departments should be used as input when you're creating an Enterprise Mobility Strategy.

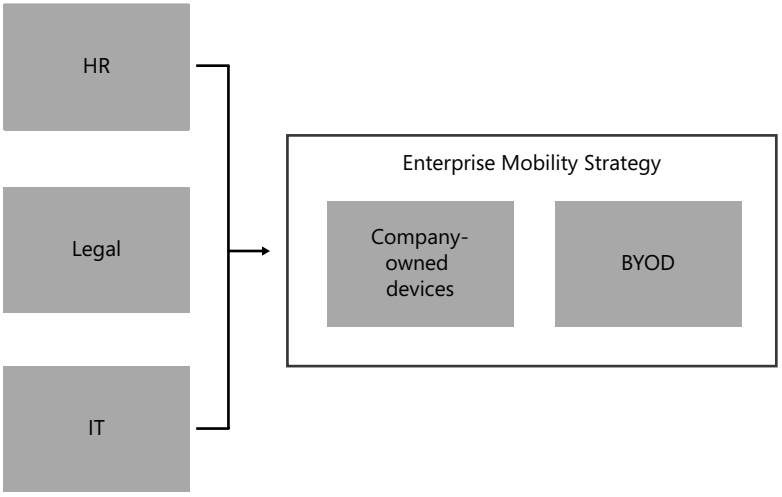

FIGURE 1-3 HR, Legal, and IT must review the enterprise mobility strategy

Awareness is an important aspect of BYOD. Employees need to be made aware of any legal risks involved in using their own devices for work-related tasks. For example, when employees travel internationally, their devices might be subject to search or seizure by border control agents. This affects not only the employee and his device but the company as well. Part of your self-assessment for BYOD adoption is making sure that the Legal and HR departments understand these scenarios. In this case, Legal should advise HR of the fact that an employee might forfeit certain rights to her personal device when using it for work. HR should also look for issues related to:

- Off-the-clock work for hourly employees and any potential compensation claims
- Local tax considerations
- Ownership of the telephone number (for a BYOD phone)

The responsibility for the loss of data on an employee-owned device can be proactively managed via policy. However, in a BYOD scenario it becomes more of a challenge. Deleting an employee's data from a personal device could have legal implications, so your organization should build a solid BYOD policy to protect itself. You should also be aware that some employees share their own devices with family members, and the shared use of employee-owned devices is one of the most pressing BYOD issues. This issue is very difficult to mitigate with policy. An employee sharing a BYOD device with his spouse invites the potential for serious issues, such as corporate data loss or security breaches.

Another BYOD scenario that must be addressed in partnership with HR and Legal is the situation whereby employees sell or recycle their own devices after those devices have been used to access company data. A common policy and technology strategy is to enable remote wiping of the device's data and require it as a condition of program participation.

IMPORTANT **For policies to be effective, they must be well written, clearly communicated to employees, and enforced. Employees who are enrolling in a BYOD program must sign an agreement that holds them accountable for their actions.**

The synergy among the HR, Legal and IT departments will help the company to better embrace enterprise mobility and address the challenges introduced by the BYOD scenario. In summary, the role of each department in this process is as follows:

- HR is responsible for developing policies for BYOD usage, selecting the people involved in setting those policies, as well as driving the training and compliance related to policies.
- Legal is responsible for identifying the information that can be accessed by specific individuals or groups and has input into policy development.
- IT implements the policies as directed by the HR and Legal departments, choosing the tools and technologies used to deliver the services, access resources, and protect data.

Understanding the Microsoft Device Strategy Framework

Figure 1-3 introduces the concept of two types of devices: company-owned device and user-owned device. However, there are variations in both ownership and management of the devices that make it necessary to expand the BYOD scenario to include the four core scenarios shown in Figure 1-4. These scenarios comprise the Microsoft Device Strategy Framework.

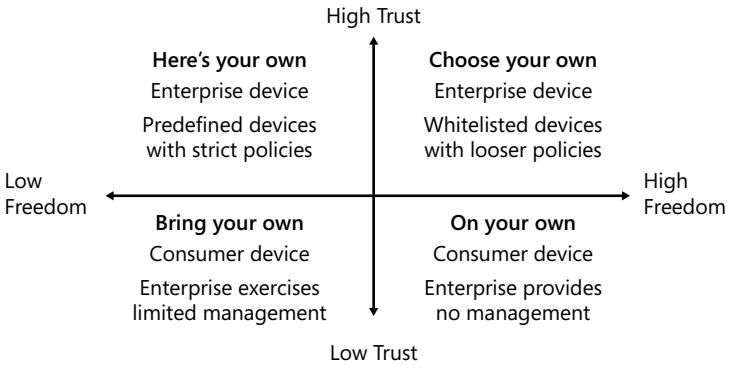

FIGURE 1-4 The Microsoft Device Strategy Framework

The scenarios shown in Figure 1-4 can be summarized as follows:

- **On your own** In this model, employees provide their own devices. There are no security policies in place, no organizational management of the device, and any device is acceptable. This is a very open approach, but it presents the highest security risk.
- **Bring your own device** This model includes two distinct variations on policy management:
  - Bring your own *unmanaged* device In this model, employees provide their own devices, but as part of the company policy, the company does not manage those devices. The employees are responsible for implementing and managing company policies on their devices. This is a flexible policy but it presents security risks; some businesses might not have the resources to manage these risks.
  - Bring your own *managed* device This is the most traditional format for BYOD. In this model, employees provide their own devices and the company enforces its policy to allow the devices to access company data. The device is fully managed by the company.
- **Choose your own device** (also called CYOD) In this model, the company provides a mobile device to employees so those employees can perform their jobs remotely. The company often allows employees to choose from a list of approved devices that are fully compatible with the company's apps and management infrastructure.
- **Here's your own device** In this model, the company has one device approved for the company's mobile platform and this device is provided to employees.

The landscape for enterprise mobility extends well beyond BYOD; you cannot assume enterprise mobility means BYOD only. There are many more elements that must be covered to completely embrace mobility and enable a mobile workforce. Each scenario has advantages and disadvantages that vary according to company requirements and goals.

MORE INFO **For more information about the Microsoft Device Strategy Framework, see the blog post by the Enterprise Mobility Team at *http://blogs.technet.com/b/enterprise-mobility/archive/2014/10/08/looking-back-and-moving-forward-with-enterprise-mobility-suite-beyond-the-byod-scenario.aspx*.**

Designing a strategy to enable a mobile workforce

This chapter has covered the factors that are driving enterprise mobility adoption and the core challenges you need to address when developing an enterprise mobility strategy. This section takes the elements shown in Figure 1-1 and explains how to use them to design an effective strategy to enable enterprise mobility.

Users

The first element is the user or employee. The user becomes a key element when companies start to move from a device-centric view to a user-centric view. Each user within your company has specific business needs; some have common business needs and some have unique business requirements. This part of the designing process is necessary to understand the user's profile. This is accomplished by defining *personas*. The following list provides examples of typical user profiles:

- **Executive** This persona expects the company to buy them whatever device they want to use as their primary device. An Executive isn't likely to be a BYOD user.
- **Mobile worker** This persona encompasses a large group of employees that are accustomed to using multiple devices.
- **Technical/field worker** This persona requires a robust device to perform their work. Usually, this type of user primarily accesses line of business (LOB) applications and email, and enters data into customer relationship management (CRM) tools.
- **Deskbound information worker** This persona uses a variety of devices and enrolls 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 worker** This persona looks to optimize their workspace, blending personal priorities with company priorities. These users might be good candidates for the BYOD program.

Keep in mind that these are just some examples of user profiles for an enterprise. Different industries and business have different roles and requirements. It is important to identify the persona and comprehend the users' needs based on their roles. You will identify these roles as part of the company self-assessment, which should be done before you start designing the enterprise mobility strategy.

You also need to consider the persona distribution, which is based on two elements: autonomy and mobility. Figure 1-5 shows the rationale behind the persona distribution.

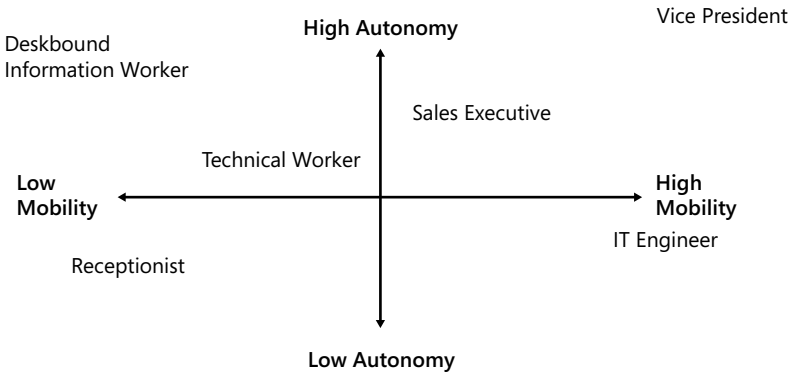

FIGURE 1-5 A persona distribution quadrant

This persona distribution relates to the user's work style and how the company can ensure that this user has what she needs to be productive. For example, some employees might always work at the same physical location (categorized as low mobility) while others might work at different branches, work from home, work from hotels, and so on (categorized as high mobility). The degree of autonomy is directly related to the balance between the freedom that the user needs to perform their business operations and the amount of restrictions added by the security policies.

Devices

Consider the type of devices that the company will allow. Access should be available from a broad set of device types, including managed devices, unmanaged devices, and consumer devices. Also, you should plan to include both Windows-based and non–Windows-based devices. Assuming your company will include a BYOD scenario, it is important to perform a survey of your employees to understand which devices they use and which operating systems they have installed on those devices.

When determining which devices will be supported by the company, carefully balance information security classification with the trustworthiness of the device and the point of connection. It is important to understand the device's capabilities and define how those devices will access corporate information. The required capabilities of each device might vary according to the company's security policy and business requirements. Figure 1-6 shows an example of some considerations regarding the device type and required capabilities. After you have defined the devices that will be supported, you need to define the required capabilities, such as data encryption, customization via policy, Mobile Device Management (MDM), and containerization.

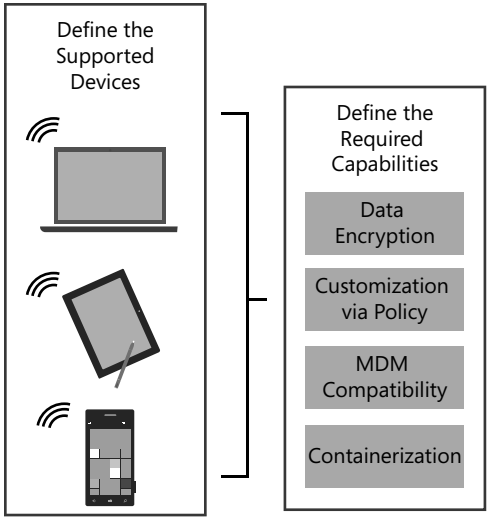

FIGURE 1-6 An example of device type selection based on required capabilities

It's important for the IT department to understand if the devices that will be supported by the company have these capabilities. Once the device type is established, you need to define the access level that the device will have based on pre-established variables. User, device, location, and data can be used as variables to define the user's experience when accessing corporate data. One variable, for example, can be the device's location. Your company policy might allow full network access only for devices that are located on-premises. When the device is located on-premises, it will have one set of policies applied to it; if it is coming from the cloud, it will have a more restrictive policy. *It is important to balance security with usability.* You don't want to enforce so much restriction that there is a negative effect on the user's productivity. If you find the right balance, you will increase productivity. Figure 1-7 shows an example of some of these variables.

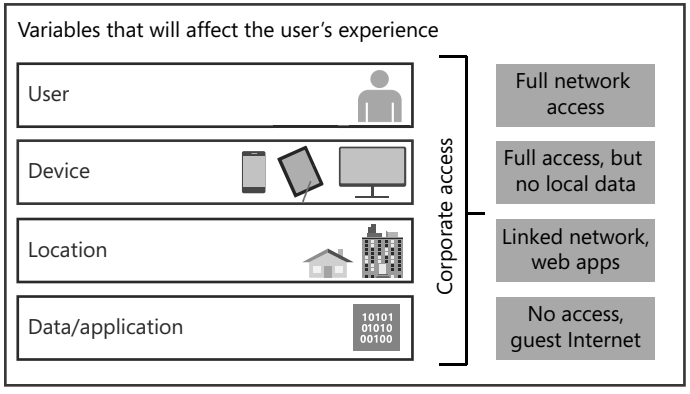

FIGURE 1-7 Examples of variables that will affect the user's experience while accessing corporate data

Using the diagram in Figure 1-7 as model, a sample policy can be defined as follows: if the device type is a Windows 8.1 phone and the device is located on-premises and it is trying to access an LOB application and the user has privileges to access that application, then the device should have full network access. Notice that each piece of the definition is connected to the next piece with "and," which makes each part of the definition a test. By creating this test, all answers to these questions must be true in order to grant full network access. These tests can vary. For example, your company might choose to use "or" instead of "and," which means only one requirement must be true to allow the device full access to the target resource.

Now that you have defined the key capabilities that are required by each device and the variables that will influence the user's experience according to the device's current state, the next important point to cover for the device is the supportability. If your company operates as a service provider, you could use a Service Level Agreement (SLA) to ensure that your users are aware of what to expect when they open an incident report with IT. An enterprise mobility strategy must include a plan to support the user's device and also set the boundaries of this support. The fact is that not all devices will be treated equally and this will impact the supportability boundaries. This should be very clear not only to the IT team but to the user as well. By knowing what to expect from support, you mitigate the possibility of user frustration when that user opens an incident report and her device has limited support.

Apps

Although the industry tends to put more emphasis on devices, apps are the main gateway to information access. If your company doesn't have mobile apps, embracing a mobile workforce won't be very productive. As part of your design considerations, you must understand the current LOB applications that are used by your employees, how these apps will behave on the different operating systems that you are about to support, as well as the user's skill level on each device that is approved by IT. When developing 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
- Perform a threat assessment 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 user's 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)

During this exercise, you will identify different gaps and each gap should be documented in detail. The output of this design consideration for apps might induce you to upgrade your server infrastructure to support this new model or adopt cloud-based apps for your mobile users.

Data

Remember, the CEO wants to enable users to be productive from anywhere, using the device of their choice, while keeping company data secure. The key to a successful enterprise mobility adoption is to allow users to consume company resources without compromising the data. The considerations regarding data protection should include:

- A security envelope to protect the data
- Safety net policies that control access and reporting
- An additional level of authentication, such as multifactor authentication
- Business-driven policies for data protection
- A classification of data according to sensitivity and business impact
- Access control to data based on identity and role
- Data encryption

You should understand how data can be protected on different platforms. Also, you should understand each platform's capabilities so those capabilities can be leveraged to protect data. Some mobile platforms will use the principle of least privilege to protect and isolate data, such as the Windows Phone security model and its use of AppContainer as a secured isolation boundary.

> ***MORE INFO*** **To better understand the Windows Phone 8.1 security model, read the white paper at *http://www.microsoft.com/en-us/download/details.aspx?id=42509*.**

While IT has full control over the data stored at the company's data center, the same level of assurance can be a challenge with unmanaged BYOD devices. How data will be stored in users' devices can directly impact how you choose to address data access and protection for enterprise mobility. Data encryption must be considered, and devices must allow IT to control when data encryption is enabled and for which types of data. Companies must review their policies and regulations to understand which types of data are allowed to leave the data-center and be at rest in remote devices' storage.

Protecting the data is not enough; you must monitor how this data has been accessed so you can take measures to mitigate potential breaches. Part of you enterprise mobility strategy includes data governance. Choosing the right management platform to monitor your data access and take actions based on what you are able to find via reporting capabilities should be a very important decision point to your company. With the assumption that users can access

data from anywhere, you must be vigilant to potential patterns that can help your company understand that an attack is in place.

Threat mitigation

After evaluating each element of your enterprise mobility strategy, you can now perform a threat modelling exercise to understand the interactions between each component and identify threats that might occur during those interactions that require mitigation. Using the core elements of Figure 1-1, you can determine who should be allowed to access the data. The first goal during threat mitigation is to reduce the attack surface by disallowing direct access to some of those elements. Figure 1-8 shows an example of the core elements of an enterprise mobility strategy. In the Before scenario, each element has direct access to the data. In the After scenario, direct access is limited to Apps only.

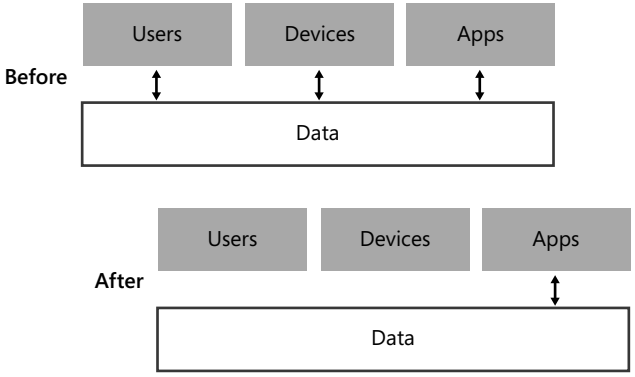

FIGURE 1-8 Reducing the attack surface by limiting direct access to the data

Another step of the threat mitigation process is to understand the risks on each interaction between these components. In Figure 1-8, for example, what risks are present when these apps have direct access to the data? You might conclude that the following actions must be performed:

- For apps to have access to data, the communication channel must be encrypted
- All mobile apps should be developed using a security development lifecycle
- Data at rest on the application server must be encrypted

To assist you through the process of understanding the risks of each interaction, you can leverage the Microsoft Threat Modeling Tool. Although this tool was created for another purpose, the rationale behind threat modeling is the same for interactions between the components of this model. Once you build the diagram and the data flows through the components, you can generate a report that will highlight the potential threats that must be mitigated. Figure 1-9 shows an example of this report.

MORE INFO **You can download the Microsoft Threat Modeling Tool at *http://www.microsoft.com/en-us/download/details.aspx?id=42518*.**

FIGURE 1-9 A report generated using the Microsoft Threat Modeling Tool

This report also categorizes the threats according to priorities, which can also help you understand which threats should be addressed first. When you finish this designing process for enterprise mobility, you should have:

- A full understanding of how your company will benefit from the adoption of enterprise mobility
- A vendor-agnostic design of your enterprise mobility solution
- A threat mitigation report with core points that must be addressed during the implementation
- A list of requirements that must be met by the vendor

This page intentionally left blank

Index

Symbols

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

This page intentionally left blank

About the authors

YURI DIOGENES is a Senior Content Developer on Microsoft's CSI Enterprise Mobility Team and has more than 20 years of experience in the IT field. He holds a Master of Science degree in Cybersecurity Intelligence and Forensics Investigation (Utica College) and has been working for Microsoft for the past nine years, including five years as a Senior Support Escalation Engineer on the CSS Forefront Edge Team. Yuri also holds an MBA and several industry certifications, including MCSE, MCTS, CISSP, E|CEH, E|CSA, Security+, Cloud Essentials Certified, Mobility+, Network+, Cloud+, and CASP. You can follow Yuri on Twitter *@yuridiogenes* or read his articles on his personal blog at *http://aka.ms/yuridio*.

JEFF GILBERT is a Senior Solutions Content Developer for the Cloud & Enterprise Division at Microsoft. From his office outside Boston, he authors cross-product solutions to IT business problems involving enterprise client management technologies, including Microsoft System Center Configuration Manager, Microsoft Intune, and Microsoft Desktop Optimization Pack (MDOP) products. In addition to local user groups, Jeff has been a speaker on enterprise client management and MDOP technologies at several conferences over the years, including the Microsoft Management Summit (MMS) and TechEd. Previous to this role, Jeff was the content publishing manager for MDOP and a senior technical writing lead for the Configuration Manager 2007 documentation team. Before joining Microsoft, Jeff was an SMS 2.0/SMS 2003 administrator with the US Army. You can follow Jeff on Twitter *@jeffgilb*.