Microsoft

Enterprise Mobility with App Management, Office 365, and Threat Mitigation

Beyond BYOD

Yuri Diogenes
Jeff Gilbert
Robert Mazzoli

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

Microsoft

Enterprise Mobility with App Management, Office 365, and Threat Mitigation

Beyond BYOD

Yuri Diogenes
Jeff Gilbert
Robert Mazzoli

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

Library of Congress Control Number: 2015951523
ISBN: 978-1-5093-0133-1

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 Support at mspinput@microsoft.com. Please tell us what you think of this book at http://aka.ms/tellpress.

Acquisitions Editor: Karen Szall
Developmental Editor: Karen Szall
Editorial Production: Christian Holdener, S4Carlisle Publishing Services
Technical Reviewer: Mike Toot; Technical Review services provided by Content Master, a member of CM Group, Ltd.
Copyeditor: Roger LeBlanc
Indexer: Maureen Johnson, MoJo's Indexing
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 improve our books and learning resources for you. To participate in a brief survey, please visit:

http://aka.ms/tellpress

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

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

http://aka.ms/tellpress

Foreword

I speak with hundreds of IT Pros and CIOs every year, and each of them has the same priority: providing their users with an iconic work environment while securing and protecting company data. Doing this has become more difficult than ever thanks to the combination of more apps/data moving to the cloud and cyberattacks becoming more destructive. It is safe to say that the traditional perimeter that was used in the past to protect company data has evaporated; this means that organizations need to fundamentally rethink how they are securing and protecting company data. Microsoft has committed itself to being an ally to the IT professionals charged with protecting the assets of their companies.

It is no exaggeration to say that, at Microsoft, we are obsessed with enterprise security. Every software company struggles with the balance between making corporate data safe from attack but accessible to the appropriate parts of the workforce—and I believe Microsoft has struck the right balance.

Teams across the company have torn down the traditional barriers that existed between products and built end-to-end solutions that are not just interoperable, but built to protect data wherever it goes. This means protecting it at multiple layers throughout the organization: protecting it at the device and apps (with Microsoft Intune), protecting the file (with Azure RMS), and protecting identities (with Azure Active Directory Premium and Advanced Thread Analytics). These products all come together to form the Enterprise Mobility Suite (EMS).

This book is written by a trio of EMS experts, and it offers an insider's look at proven, real-world actions you can take to manage your enterprise mobility needs, enable your workforce to be productive (across devices and platforms) with an iconic work experience, and help you protect your organization's assets and your workforce's privacy.

As you read, I think you'll be consistently impressed by the ways you can leverage EMS's powerful ability to deliver an incredible work experience for your users that correctly balances between user empowerment and data protection. To do this, we have engineered EMS and Office 365 to be used together.

The value and power of what we've built is widely recognized by the IT industry —EMS has already outgrown its competitors and continues to regularly add more features and functionality. We are committed to continuing to build, refine, and deliver the tools you need to protect your organization and empower it to do more.

Brad Anderson, Microsoft Corporate VP, Enterprise Client & Mobility

@InTheCloudMSFT

This page intentionally left blank

Introduction

Enterprise mobility management is one of the fastest-growing areas in the Information Technology field, and having a solid understanding of the newest features and capabilities is an important part of configuring and managing mobile devices. This book continues forward from the information covered in *Enterprise Mobility Suite: Managing BYOD and Company-Owned Devices* (Microsoft Press, 2015) and covers the fundamentals and capabilities of several Microsoft mobility management resources; the newest mobile application management features in Microsoft Intune, Microsoft Advanced Threat Analytics (ATA), and Mobile Device Management for Office 365 (MDM for Office 365). Throughout this book, we guide you through all the areas associated with planning, designing, and implementing these mobility management solutions.

Is this book for you? This book is for enterprise IT professionals who are responsible for implementing and managing mobility management technology as well as professionals charged with identifying and mitigating networking threats to on-premises networks. It is also meant to provide foundational expertise to IT professionals who aren't already familiar with these solutions or just want to learn more. We assume that the readers are familiar with the primary components of the Microsoft Enterprise Mobility Suite (EMS) and Office 365. It is also helpful to have basic knowledge about network-security principals and network-infrastructure components.

The scenarios described in this book are meant to be an end-to-end journey for each of the mobility management solution areas. They start with understanding overviews of each solution and then move on to implementing specific features and capabilities in the example organization. After completing the example scenarios, you'll have learned how to

- Manage and publish mobile applications, and deploy them to mobile devices and computers
- Deploy and configure the ATA Center and Gateway, including configuring reports to help identify suspicious activities
- Activate and configure MDM for Office 365, including enrolling and managing mobile devices

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 the other Microsoft colleagues who contributed by reviewing this book: Gershon Levitz, Ophir Polotsky, Benny Lakunishok, Michael Dubinsky, Simon May, Sonia Wadhwa, Stacia Snapp, Owen Yen, Paul Mayfield, Joey Glocke, Rob Stack, and Karthika Raman. In addition:

Yuri I would like to thank my wife and daughters for their support and understanding, my great God for giving me strength and continuing to guide my path, my friends and co-authors Jeff Gilbert and Robert Mazzoli (you guys rock!), the Microsoft ATA Team in Israel for the endless support on this project, 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 I would like to thank my wife, Chrissy, and kids, Nick, Haylee, Jackson, and Jillian for their love, patience, and unending support and encouragement throughout the long hours required to author content for a technical book of this depth. Also, thanks to my co-authors who kept me motivated to write and who I can count on every day for expert counsel and advice. Thanks also to the other Microsoft enterprise client management engineering team members who made themselves available for my never-ending stream of questions and clarifications.

Robert I would like to thank my daughter, Alyssa, for inspiring me to follow in her footsteps and become a published author; Barbara for being the love of my life and for all her patience and understanding; Bruna and Luciano for the use of their kitchen table and all the wonderful Italian meals that fueled my writing; my co-authors Jeff Gilbert and Yuri Diogenes for their ongoing friendship, guidance, and motivation; and "all" my parents (Constance, Claude, Henri, and Kathy) for a lifetime of love and support.

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!

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/EM2/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

Understanding Microsoft enterprise mobility solutions

Enterprise mobility management solutions aren't as simple anymore as connecting a few mobile devices to an email server or allowing some users to access company resources via a remote connection. Today's IT departments must support a much more robust and comprehensive user experience for modern employees. Users expect, and often even demand, application-feature and data-access parity between their mobile devices and the devices they use at the office. Add in the new challenges that IT departments face with managing cloud-computing services, user identity, applications, data security, and threat mitigation, and the enterprise mobility management landscape becomes much more complex and difficult to deploy and manage.

This chapter explains how Microsoft enterprise mobility solutions address these areas and covers the basics of enterprise mobility management. It also covers considerations for selecting and deploying these solutions, as well as introducing a sample enterprise mobility management scenario that will be used throughout this book.

Enterprise mobility management concepts

In enterprise IT management, companies are fully embracing the modern "work anywhere, from any device" vision. Trends like *bring your own device (BYOD)* and *mobile application management (MAM)* aren't just buzzwords or passing fads likely to fade out after a year or two. These concepts are part of the larger modern IT strategy supporting the consumerization of IT and the empowerment of users. Central to this strategy are cloud services, such as Microsoft Azure Active Directory and Microsoft Office 365. Leveraging the computing scale and ubiquity of access that these and other Software as a Service (SaaS) platforms provide to mobile devices and users requires planning and considering things from a different perspective than in the past.

Enterprise mobility management isn't just about connecting mobile devices to cloud services or resources. In fact, it's less about *devices* and more about *people*. Forward-looking organizations aim to empower employees and increase their productivity; the devices (mobile or not) they use are merely tools to help accomplish their work. This paradigm shift from a *device-centric* management structure to a *people-centric* management structure is significant. All the components that enable mobile productivity in an enterprise mobility management solution must have a people-centric architecture that aligns with enabling this vision. Finding the proper balance where employee empowerment and productivity meet the business needs of your organization is the crucial requirement for any enterprise mobility management solution.

With this vision in mind, be aware that a well-designed enterprise mobility management solution must address several key areas of the modern workplace, as shown in Figure 1-1.

- Users
- Devices
- Apps
- Data
- Protection

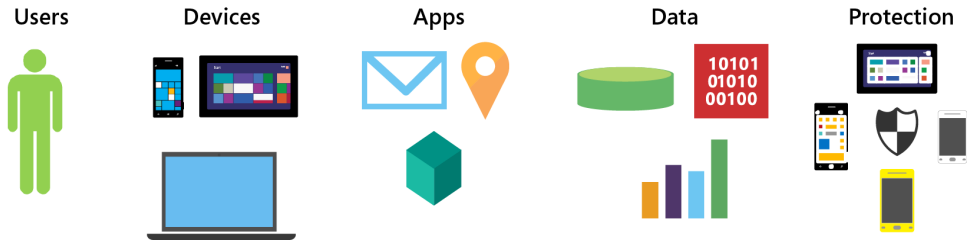

FIGURE 1-1 Elements of enterprise mobility management

> ***MORE INFO*** **For more information about why organizations should embrace enterprise mobility solutions, read Chapter 1 of *Enterprise Mobility Suite: Managing BYOD and Company-Owned Devices* from Microsoft Press at *https://aka.ms/EMSdevice/details*.**

Users

The first and most important element of the enterprise mobility management solution is the user or employee. Without the employee, the IT infrastructure and management costs to enable enterprise mobility are expensive monuments to best intentions. The enterprise mobility solution must support effective ways to manage user accounts and make it easy for employees to access resources. If user identity is hard to manage by IT administrators, or if employees are required to take convoluted steps to gain access to devices or company resources, the enterprise mobility

management solution becomes an obstacle instead of an effective productivity management tool. As most experienced IT administrators have learned, workplace technology obstacles invite shortcuts, workarounds, and questionable data-protection practices.

Effectively managing user identity is critical to enabling cloud-based applications and data resources spanning multiple services or locations. Efficiently verifying that users are who they claim to be is essential to protecting resources and making the mobile experience feel like the traditional workplace experience. Keep in mind that employees with different types of roles and responsibilities, and even different geographic locations, often have unique requirements across all the areas of enterprise mobility management.

Devices

The rapid pace of technological advancement has changed the modern workplace from one of stationary workstations and company-issued devices to one containing a mix of all types of mobile computers and Internet-connected devices. This change is driving the BYOD trend across all markets, and industries and organizations must adapt to this new challenge. Using their personal mobile devices—such as smart phones, tablets, and laptops—employees are increasingly mixing their personal lives with their work responsibilities. As a result, IT departments are tasked with managing an ever-expanding collection of different mobile hardware, operating systems, and vendor-specific architectural requirements.

It's critical that organizations fully understand the capabilities and limitations of each type of device and how they will support each one. Only then can organizations define and configure the necessary enterprise mobility management features that support both the employee's needs and the organizations business requirements.

Apps

Apps are the centerpiece of most business requirements and the portal for information access for modern organizations. Though managing different device types creates new administration challenges, managing a mixture of commercial and customized line-of-business (LOB) apps can be equally challenging. 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.

How to properly install and manage these apps depends on several factors. 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. Mobile application management will be covered in more depth in Chapter 2, "Introducing mobile application management with Microsoft Intune," and Chapter 3, "Implementing MAM."

Data

Working from a mobile device from any location really means accessing data from anywhere. 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.

Depending on your 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.

Protection

Protecting mobile devices and company data from threats is just as important as securing data access. No matter how carefully planned security is, all levels of mobile device security are potentially vulnerable to a wide variety of malicious activity. These vulnerabilities include threats to company data, personal information, and even user identity.

Depending on the enterprise mobility management solution, preventing risk and protecting mobile devices from these threats can be included as tightly integrated features or standalone services. Understanding how these solutions address potential gaps in threat mitigation is extremely important to effectively protecting mobile devices that are coming from the cloud or located on-premises. Threat protection and mitigation will be covered in more depth in Chapter 4, "Introducing Microsoft Advanced Threat Analytics," and Chapter 5, "Implementing Microsoft Advanced Threat Analytics."

Microsoft enterprise mobility solutions

Microsoft has aggressively pursued a strategy of "mobile first, cloud first" in their enterprise mobility management vision. This vision is centered on helping organizations enable their users to be productive on the devices they prefer, while protecting company resources. Central to this vision is the concept of *balance*—balancing the financial and data-security needs of the company with the productivity and privacy needs of users. Finding an appropriate balance often means splitting authority between the company and users, and keeping added management complexity to a minimum to ensure satisfaction and compliance.

Instead of piecing together parts of existing on-premises products and attempting to update and rebrand them as cloud services, Microsoft chose to design an enterprise mobility management solution from the ground up and leverage the powerful features of its proven cloud services, such as Azure and Office 365.

Microsoft Enterprise Mobility Suite

The Enterprise Mobility Suite (EMS), shown in Figure 1-2, is a comprehensive set of cloud services and on-premises technologies designed to extend user identities to the cloud, manage mobile devices and apps, increase user productivity through native support for Microsoft Office apps and support for thousands of SaaS applications, and protect files accessed and stored on managed devices.

EMS comprises the following products:

- Microsoft Azure Active Directory Premium
- Microsoft Intune
- Microsoft Azure Rights Management
- Microsoft Advanced Threat Analytics

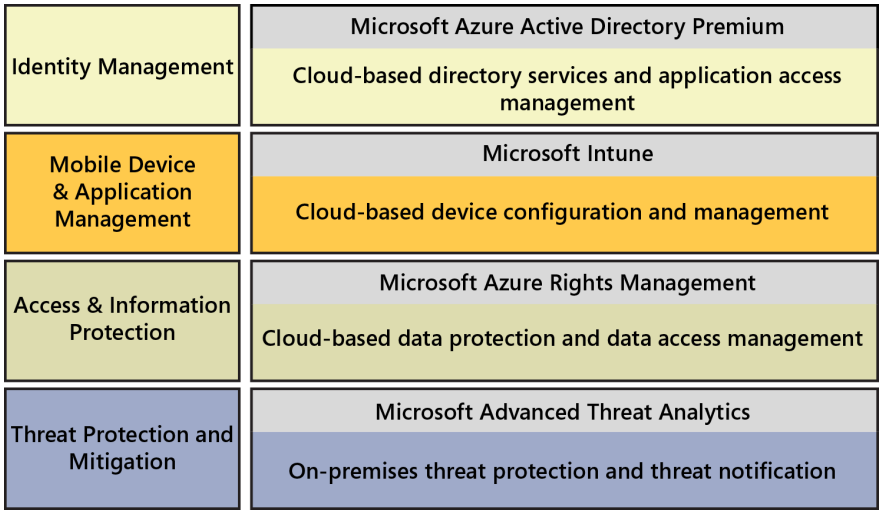

FIGURE 1-2 Enterprise Mobility Suite products

IMPORTANT **This book doesn't cover all the products included in EMS in depth. Instead, it focuses on several key features and capabilities of some EMS services, such as mobile application management (without device-enrollment requirements) and threat protection using Advanced Threat Analytics. It also covers the enterprise mobility management features of Microsoft Device Management (MDM) for Office 365 that aren't included in EMS. You can learn more about the products included in EMS in the first book in this series, *Enterprise Mobility Suite: Managing BYOD and Company-Owned Devices (https://aka.ms/EMSdevice/details)*.**

Azure Active Directory Premium

Azure Active Directory (Azure AD) Premium is a Microsoft cloud-based service that provides comprehensive user identity and application access management capabilities. Built on the rich set of directory-service features of Azure AD that is included in all Microsoft Azure subscriptions, the Azure AD Premium subscription includes additional capabilities for enterprise-level identity management. One of the most popular features of Azure AD Premium is its integrated single sign-on (SSO) support for thousands of popular Software as a Service (SaaS) apps. This means that instead of users having to use multiple sets of user names and passwords to access apps such as Salesforce, Concur, or Workday, they can use a single user name and password for a consistent experience across every app and device.

In addition to the features in the Azure AD Free and Basic subscriptions, the Premium subscription includes the following:

- Self-service group management that users can use to create and manage customized user groups
- Advanced security reports and alerts based on machine-learning that organizations can use to monitor and protect access to cloud applications
- Multi-factor authentication (MFA) that supports configuring user verification steps in addition to a single user name/password authentication process
- Microsoft Identity Manager (MIM) support option you can use if you need to configure additional on-premises hybrid identity services
- Password reset with write back for user self-service password management with on-premises directory services
- Azure AD Connect Health to monitor on-premises identity infrastructure and synchronization services available through Azure AD Connect

Microsoft Intune

Microsoft Intune is another Microsoft cloud-based service that provides mobile device management (MDM), mobile application management (MAM), and Windows PC management capabilities. Supporting Android, iOS, and Windows-based devices, Microsoft Intune also can be used as a standalone cloud service or connected to an existing on-premises Microsoft System Center Configuration Manager 2012 R2 or later deployment. Additionally, Microsoft Intune provides the infrastructure support for enterprise mobility management features included with Office 365.

Microsoft Intune supports a comprehensive mix of MDM and MAM capabilities, including

- Simplified device enrollment for Android, iOS, and Windows devices
- Mobile device management through configuration and compliance policies
- Device access profiles for managing access to virtual private networks, wireless networks, email servers, and certificate-controlled resources