

9 reasons why Microsoft customers choose MobileIron to close the gap

TABLE OF CONTENTS

Introduction 3

Nine Reasons Why
Microsoft Customers
Choose MobileIron 4

Security for a Modern
Digital Workplace 13

Conclusion 15



INTRODUCTION

Organizations considering making the move to a Microsoft bundle with Intune should take a close look as to what that means, including limits on security and operational flexibility that can slow growth plans for a modern digital workplace. We have identified nine reasons why many Microsoft customers choose MobileIron to extend their security through a mobile-centric zero trust approach.



NINE REASONS WHY MICROSOFT CUSTOMERS CHOOSE MOBILEIRON

Here are nine reasons why enterprise customers have chosen MobileIron to extend their security and better align with their organizational goals:

- 1 Hybrid enterprises need the flexibility that MobileIron provides
- 2 It's more than just a Microsoft world
- 3 End-user experience and choice matter
- 4 Demand identity, device, app and data security—all in one
- 5 Eliminate passwords today with MobileIron's device -as-identity approach
- 6 MobileIron integrates well with best of breed technology partners
- 7 The high cost and complexity of switching solutions
- 8 Choice of on-prem or SaaS deployments
- 9 Choose a proven leader, acknowledged for driving the convergence of mobility, security and identity

1 Hybrid enterprises need the flexibility that MobileIron provides

Modern enterprises are adopting a variety of SaaS apps across every function. As organizations shift from the on-premises datacenter to SaaS apps, they need a security platform that will accommodate all their needs, while still securing on-prem apps.

Unified security for all apps

Organizations that use a range of SaaS apps from many different vendors in addition to Microsoft require both a unified and equivalent compliance and security approach. Azure AD conditional access decisions cater to apps that support modern authentication, which makes Azure AD an incomplete unified security solution for all apps—legacy and modern.

Secure business-critical on-prem apps, data, devices and identity—all in one

Many organizations want to keep their business-critical and proprietary apps on premises. They choose MobileIron because we provide a per-app VPN that secures and encrypts data from the device to the resource(s), which means secure and seamless end-user access to data from any device, anywhere.

A consistent password-less experience for all apps

Organizations see a helpdesk reduction of 50% in password resets after deploying MobileIron Access with Zero Sign-On. Once they've experienced MobileIron, users have a hard time going back to an experience that doesn't provide password-less for all apps—on any device.¹

¹ Percentage based on 2019 MobileIron assessments.

Greater admin ease of use

MobileIron offers easy app configuration and distribution throughout your entire organization, including the ability to delegate admin control for non-corporate wide access and control.

Helpful cloud migration tools

MobileIron gives customers and partners the ability to choose the deployment model they want, such as on-premises, in a data center provided by a partner, or via the cloud. Customers can move devices from their MobileIron Core implementation on-premises to MobileIron Cloud without impacting the end-user.

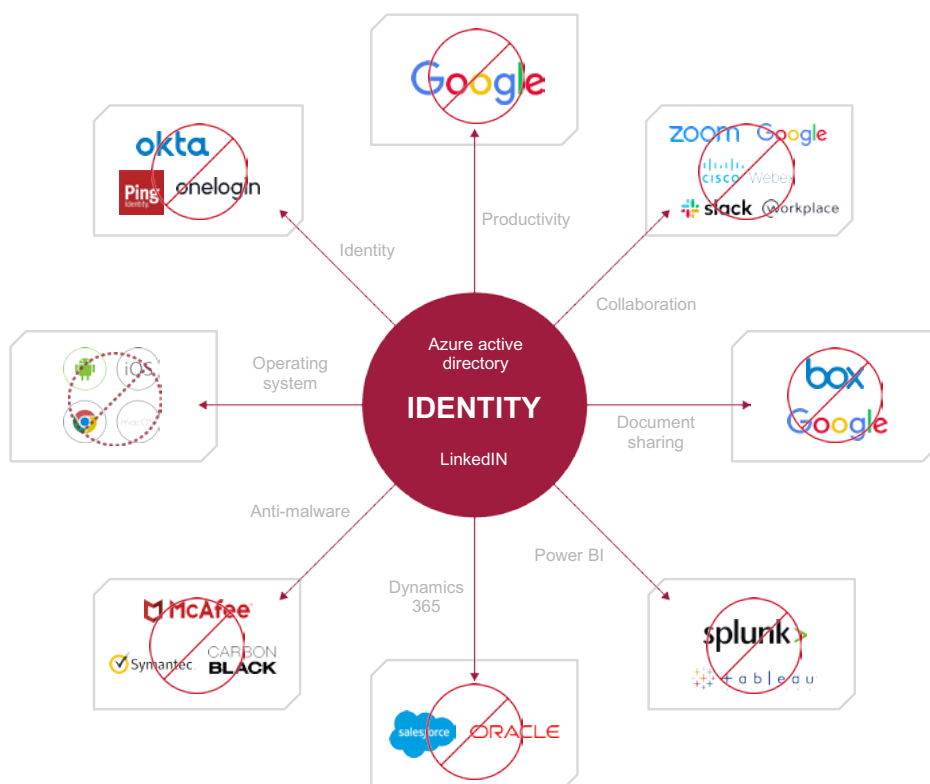
2 It's more than just a Microsoft world

Are you prepared to rely on Microsoft for everything—email, office collaboration, AAD, identity, security, mobility and device infrastructure—does that reduce your purchasing options if Microsoft changes its product offerings and product bundles in the future? Are you prepared for bundle creep—regardless if you need everything in them? If you lock into Microsoft for everything, you may be locked into every future change in Microsoft's technology roadmap.

Microsoft's integrations may be tighter and end-user experiences smoother with their own solutions, but for competing best-of-breed apps and services that are widely deployed at many companies, the end-user experience is not the same.

Microsoft's Approach: Locking out best-of-breed tools

Are you ready for only Microsoft to guide your company's operational and security direction now and into the future?



3 End-user choice and experience matter

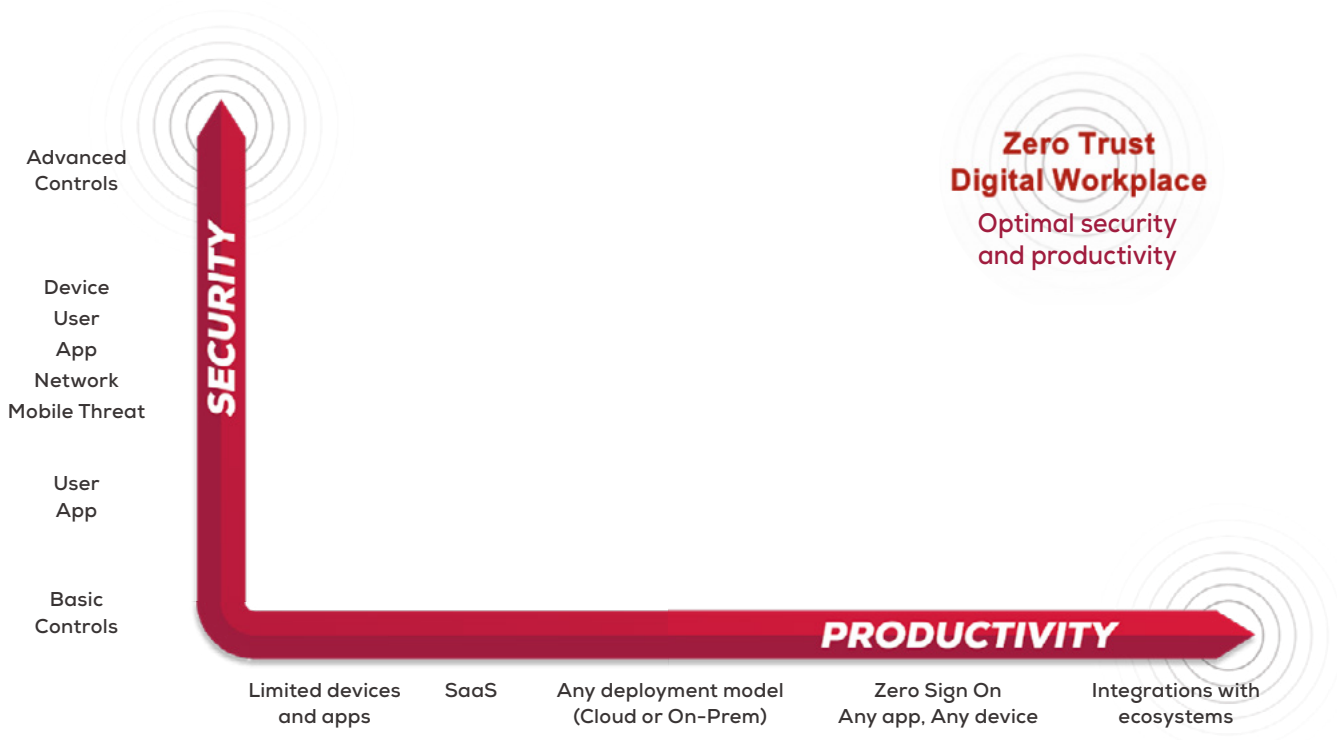
If providing employees device and app choice matters to an organization as much as the seamless experience to access them, you look at the big picture differently. That's why MobileIron provides the better approach. From the simplest onboarding to the best on-device experience, solutions that offer flexibility for productivity that affects the bottom line—make sense.

Address the needs of the Modern Digital Workplace

If providing employees device and app choice matters to an organization as much as the seamless experience to access them, you look at the big picture differently. That's why MobileIron provides a better approach. From the simplest onboarding to the best on-device experience, solutions that offer flexibility for productivity that affects the bottom line—make sense and address the needs of today's modern digital workplace.

Allowing users to work from any device, using any app, from any location, over any network is key to the success of the Modern Digital Workplace. Only adaptive security will secure business data across any device and app that employees choose—without affecting the user experience. If security gets in the way of productivity, your users will find a way around it, and it won't be a secure one.

This diagram shows the continuum of productivity and security in the workplace. The more advanced controls you have, the stronger your security as you head toward Zero Trust. The more apps and services that improve productivity, the closer you are to becoming a Modern Digital Workplace. The secure sweet spot is the upper right corner, optimizing both as you head toward a Zero Trust Digital Workplace.



Zero Trust Security

Secure access that's determined by a "never trust, always verify" approach, requires verifying the device, user, apps, networks and presence of threats before granting access—with constant enforcement.

A Zero Trust Digital Workplace User Experience

ELIMINATE PASSWORDS. With Zero Sign-On, your mobile device is your ID and secure access for the enterprise—no more hassle of remembering and typing passwords or the breach risk they represent. (See Reason 5)

SEAMLESS ONBOARDING for iOS, Android, macOS, tvOS, and Windows10. Intune puts the burden on the end-user to get through the entire, non-intuitive enrollment flow. We estimate that it takes an admin expert 24 minutes to onboard one device using Intune.² With MobileIron, end-users don't have to go through cumbersome enrollment flows. (See Reason 7)

Critical use cases MobileIron supports to close the Intune gap today

MobileIron is the best solution for organizations that need to manage devices beyond Windows and iOS by providing support for all possible end-user device use cases.

- **Privacy with Android knowledge worker (Work Profiles on fully managed devices).**
If you own the device but want to support the end user to have a private side of the device, you can securely enable that to maintain user privacy.
- **Control FOTA for Samsung and Zebra devices (firmware-over-the-air)**
Get granular control of scheduled updates to these rugged devices to efficiently manage uptime and avoid interfering with business. Intune currently does not support manufacturer-specific Android updates.
- **MDM vs full macOS**
MobileIron offers a comprehensive MacOS solution, including both modern management and full MacOS control for functions like creating shortcuts on the desktop and Safari bookmarks.³

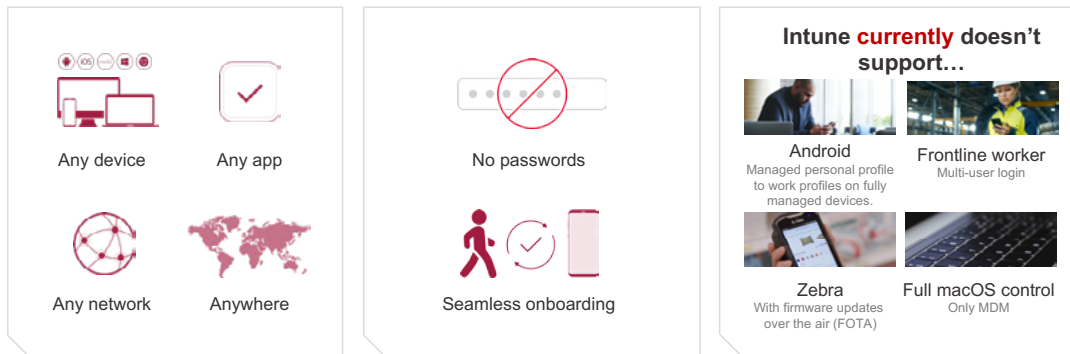
**SEE HOW WELL
MOBILEIRON
STACKS UP AGAINST
MICROSOFT AND
JAMF IN GARTNER'S
REPORT**

² End-user Intune enrollment instructions for IT administrators, Microsoft, January 2017.

³ Solution Comparison for Four macOS Management Systems, Gartner Research, Michael Disabato, March 11, 2019.

NINE REASONS WHY MICROSOFT CUSTOMERS CHOOSE MOBILEIRON

Customers choose MobileIron for user choice, user experience and support of key use cases



4 Demand all-in-one security: identity, device, app and data

For the highest security posture, companies demand that user and device authentication, device posture, app and data security are managed in a single product. You need a framework that will protect your data the ways it's being accessed and used—no matter where it is, or who owns the devices and services involved. This is where data containerization and integrated threat defense capabilities—implemented on-device, closest to where the data lives—are critical.

Mobile-centric, zero trust security closes the gaps

When secure access is determined by a "never trust, always verify" approach, that's mobile-centric, zero trust security. It requires verifying the device, user, apps, networks and presence of threats before granting access—with constant enforcement.



MobileIron helps transform your device into your secure ID, enabling secure access to the enterprise. These critical capabilities lay the groundwork for the expanded business use cases that Intune can't fully support.

Where Microsoft falls short today

- 1. Addressing security and compliance requirements:** The public sector and many regulated industries have stricter security and compliance requirements that they must meet. MobileIron supports many certifications that Microsoft currently does not support.
- 2. Protection with privacy:** Our per-app VPN provides a clear distinction between personal and work by surrounding only corporate apps, not employees' personal ones. Microsoft currently does not have or include a VPN in their bundle.
- 3. Activation and protection.** Because MobileIron is on-device, MobileIron Threat Defense is automatically activated when a device is enrolled for 100% adoption. Using a third-party mobile threat defense solution with Microsoft requires end-user activation, resulting in lower adoption rates.
- 4. More device, threat and network signals** create higher zero-trust security. MobileIron provides a more robust conditional access for a zero sign-on experience with minimal friction to the end-user experience.

5 Eliminate passwords today with MobileIron's Device -As-Identity Approach

The number of systems and apps most businesses use is on the rise—each requiring its own secure authentication. Relying on passwords is not only frustrating for users but a burden on IT. Passwords are also notoriously unsecure. MobileIron, however, combines zero sign-on capabilities with our mobile-centric, zero trust approach that automatically validates every user, device, app, network, and threats before greenlighting access — all without requiring a password.

CERTIFICATIONS MOBILEIRON SUPPORTS

FIPS 140-2 VALIDATED
CONTAINER

COMMON CRITERIA
FOR MDMP V3.0

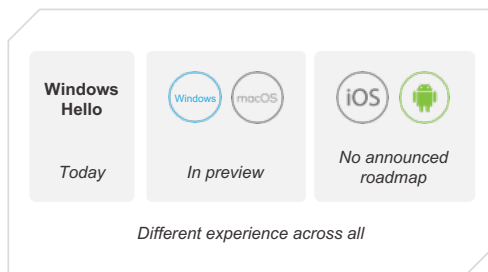
DISA STIG

CCN QUALIFIED

PASSWORD-LESS EXPERIENCE.

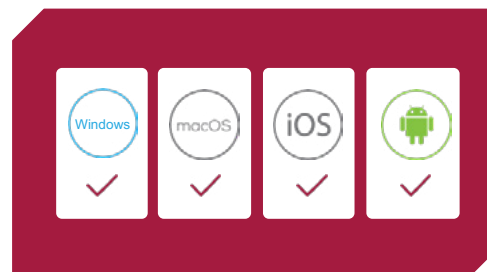
ZERO SIGN-ON FOR ALL APPS
IS ONLY POSSIBLE WITH
STRONGER CONDITIONAL
ACCESS.

MSFT password-less approach is ONLY desktop Everything else is still passwords



⚠️ High friction ⚠️ Low security

Zero Sign-on using Device-as-identity



✓ Low friction ✓ High security

Where Microsoft currently falls short:

- Microsoft's password-less approach is focused primarily on the desktop, namely Windows 10.
- With Windows 10, Windows Hello for Business has been available since 2015, but the adoption rate for enterprises has been low because it requires companies to buy into a Microsoft lock-in strategy.
- With desktops that don't support Windows Hello (macOS and Windows), their password-less solution requires a separate app (Microsoft Authenticator) to install, pair and register, which makes for a poor end-user experience.
- Microsoft still relies on a password for applications on iOS and Android today.

WITH ANDROID AND IOS, MICROSOFT DOES NOT HAVE A COMPLETELY PASSWORD-LESS EXPERIENCE.

81% OF BREACHES ARE DUE TO POOR PASSWORDS⁴

6 MobileIron integrates well with best of breed technology partners

The Modern Digital Workplace needs to be able to choose the right tools and best-of-breed solutions to properly secure the way employees want and need to work. Integrating with these best of breed partners is critical.

Tighter integration with over 380 technology applications

- It's critical that your security platform uses a standards-based approach and integrates with a wide set of IT systems that allows you to customize.
- Organizations that choose MobileIron UEM over Intune appreciate the tighter integration that MobileIron has created with our over 380 ecosystem partners, including ServiceNow, Splunk and many more.



The following are just a few of the major vendors with whom MobileIron has integrations:

- Leading Identity vendors: Okta
- Certified FirstNet network vendors: NetMotion Mobility
- Service management tools: ServiceNow
- Security information and event management tools: Splunk

None of these vendors have integrated with Microsoft Intune.

7 The high cost and complexity of switching solutions

The complexity of an Intune integration is significant since there's no easy tool to migrate—meaning everything you've set up with MobileIron or another vendor will have to be done all over again with Intune.

We've estimated the tasks and time involved to complete a migration from MobileIron to another UEM provider such as Intune. The price tag comes to about \$100-\$150 per person, per device.⁴

\$100-\$150
PER PERSON/DEVICE
ESTIMATED COST OF
INTUNE MIGRATION

The Cost Factors in an Intune Migration

- Microsoft or Partner Consulting Services
- IT hours to train on Intune
- IT hours to setup new instance of Intune
- IT hours to setup migration process (full device re-registration)
- Number of devices IT can move per hour
- Number of hours to develop & conduct end-user training
- Employee time to migrate their device
- Migration failure rate
- Employee and IT time to remediate failed migration
- Employee training time on new system

Unbundle the Microsoft bundle—is it more than you need?

The complexity of Microsoft licensing and their bundling strategy requires investigating to see if what they offer really aligns with your company's needs. Several customers have found that they are paying for functionality they neither want or need, diminishing the bargain of the bundle.

The Cost of Switching

A Fortune 500 company with 17K+ devices potentially saved almost \$2M when staying with MobileIron, while a large services provider with almost 90K devices could save almost \$9M.⁵

Moving to Intune is a costly and heavy lift

IMPACT TO IT

Complete re-architecture of mobile infrastructure:

- Build new policies,
- Manually add all settings
- Security re-Review of app tunneling
- VPN and other solutions
- Full end-user re-training
- Global education program
- Helpdesk support for device migration.

IMPACT TO USERS

Highly disruptive:


- Complete device retire and re-registration
- Manual acceptance of MDM Cert. (30% failure rate)
- Devices using Apple Business Manager must be FACTORY RESET.
- All end users must be re-trained on new system.

8 Choice of on-prem or SaaS deployments

Most Fortune 2000 companies were not born in the cloud and will need to have the flexibility to continue to deploy UEM on-premises and/or in the cloud. Many organizations aren't allowed or choose not to send their business-critical and proprietary apps to the cloud. Microsoft doesn't give them that option today.

UEM Deployment Options

When deployed within a network infrastructure, MobileIron UEM can adhere to strict corporate security policies by storing all data on site. It can also run on virtual environments, which allows for seamless deployments on several different setups.

UEM	DEPLOYMENT AS A SERVICE	DEPLOYMENT ON-PREMISES
MICROSOFT INTUNE	✓	
	✓	✓

9 Choose a proven leader, acknowledged for driving the convergence of mobility, security and identity

Industry analyst leadership

MobileIron, named a Leader in Gartner Magic Quadrants for 9 consecutive years⁶, has enjoyed a strong standing among industry analysts for years. Most recently in Gartner's 2019 Magic Quadrant Critical Capabilities, MobileIron ranks higher than Microsoft in three out of four Gartner use cases and five out of eight critical capabilities. MobileIron was also the only UEM vendor in the study in addition to being named a strong performer in the most recent "2019 Forrester Zero Trust X Wave."⁷

⁶ 2019 Gartner Critical Capabilities for Unified Endpoint Management (UEM), MobileIron.

⁷ The Forrester Wave™: Zero Trust Extended Ecosystem Platform Providers, Q4 2019, MobileIron.

SECURITY FOR A MODERN DIGITAL WORKPLACE

Work the way you want: any device, any app, anywhere

The modern digital workplace needs to have the most flexibility in choice of applications and devices with the best end-user experience. And that takes a solution developed with mobile-first design thinking. Driving digital transformation with a desktop based orientation constantly plays catch up as it runs into restrictions and limitations around use cases that MobileIron has long since addressed. MobileIron's orientation from the start has and will always be mobile. It's why over 19,000 customers choose MobileIron as their partner to stay secure in a perimeter-less world.

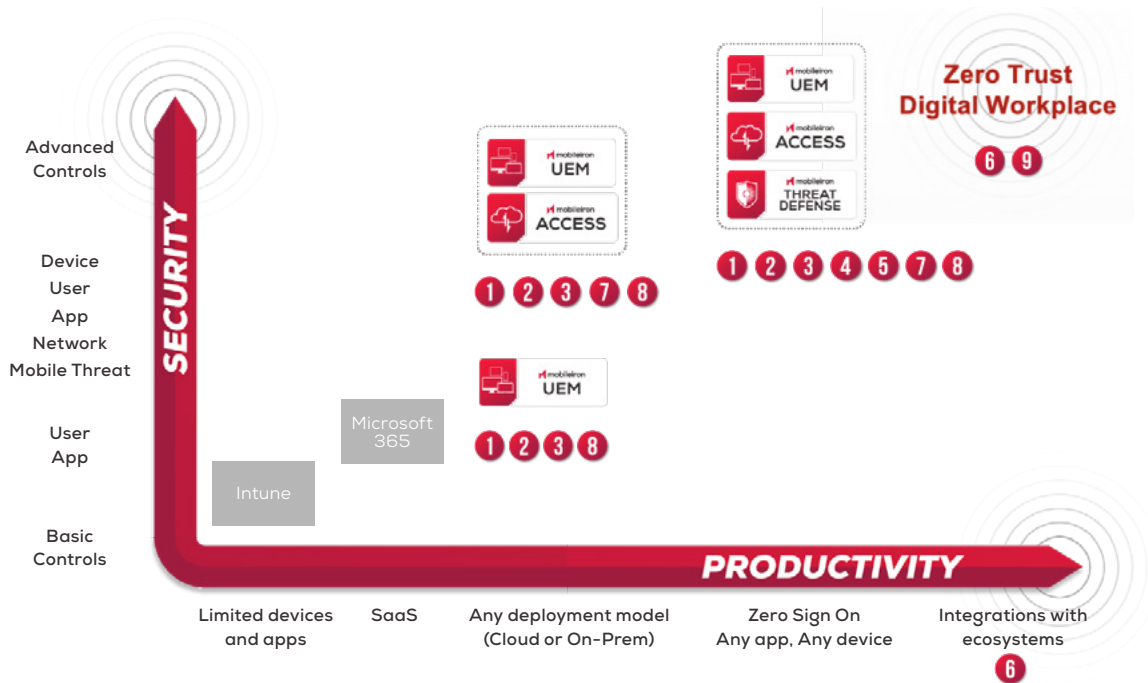
MobileIron can take you the distance

Your security and productivity are on a continuum that's affected by the choices you make with Microsoft and MobileIron. The nine reasons clearly show that MobileIron helps take your organization toward the secure sweetspot—closer to achieving the goal of the Zero Trust Digital Workplace.



Accelerate and secure your hybrid digital workplace journey with MobileIron

As you can see, the only way to achieve a zero trust digital workplace is with MobileIron. The rest leaves you settling for “good enough” in terms of both security and productivity — and with consequences that affect your digital roadmap and growth strategy.



- 1 Hybrid enterprises need the flexibility that MobileIron provides
- 2 It's more than just a Microsoft world
- 3 End-user experience and choice matter
- 4 Demand identity, device, app and data security—all in one
- 5 Eliminate passwords today with MobileIron's device -as-identity approach
- 6 MobileIron integrates well with best of breed technology partners
- 7 The high cost and complexity of switching solutions
- 8 Choice of on-prem or SaaS deployments
- 9 Choose a proven leader, acknowledged for driving the convergence of mobility, security and identity

CONCLUSION

When technology bundles are pitched as a value that “includes security and management for free!” It’s only natural that some alarms go off. Committing to a Microsoft-only world comes with sacrifices. Many customers have selected MobileIron or added it to close the gaps that a Microsoft-only stack couldn’t address. The reasons are clear:

- **Hybrid enterprises need more:** Organizations that use a range of SaaS apps beyond Microsoft require both a unified and equivalent compliance and security approach.
- **Their digital world goes beyond Microsoft:** Deploying Microsoft for everything limits purchasing options for renewals and locks you into shifts in their technology roadmap.
- **The importance of end-user choice and experience:** Working on any device with any app from any vendor requires a flexibility that only MobileIron can provide.
- **Costly migration:** The complexity of switching from MobileIron to another UEM like Intune has a price even if the UEM solution is “included for free.” We estimate such migrations cost \$100-\$150 per user, per device.

This ebook shows what switching to a Microsoft-only bundle would mean for your company. Only MobileIron can provide a comprehensive solution that fits your needs and critical use cases without forcing you to incur additional and unnecessary costs.

[LEARN MORE](#)

