

# TechEd

## India 2014

Learn. Connect. Explore.

# Enterprise Mobility Services

**MS Anand**

Technical Architect Evangelist

**Anirudh Singh Rautela**

Enterprise Mobility Business lead - India

The challenges we face today in  
keeping users productive while  
protecting company information

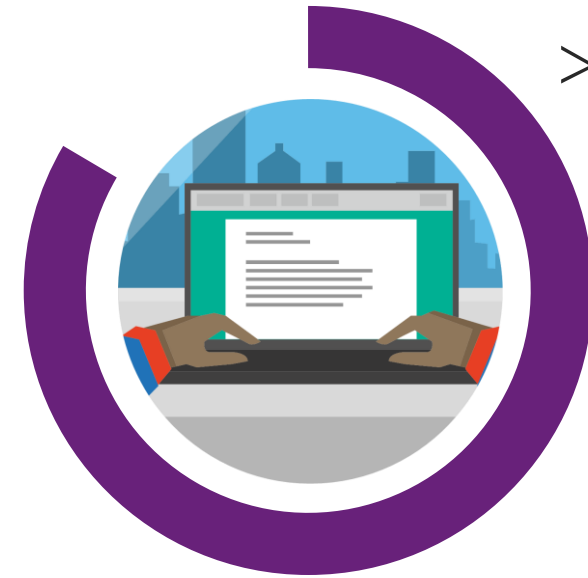
# Mobility is the new normal



52% of information workers across 17 countries report using three or more devices for work\*



90% of enterprises will have two or more mobile operating systems to support in 2017\*\*



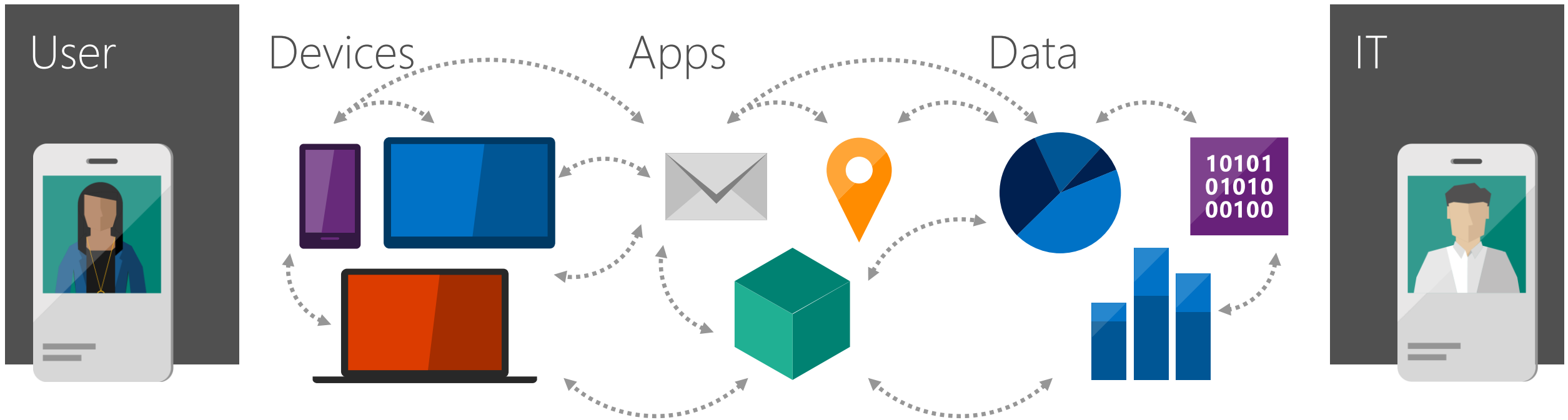
>80% of employees admit to using non-approved software-as-a-service (SaaS) applications in their jobs\*\*\*

\* Forrester Research: "BT Futures Report: Info workers will erase boundary between enterprise & consumer technologies," Feb. 21, 2013

\*\* Gartner Source: Press Release, Oct. 25, 2012, <http://www.gartner.com/newsroom/id/2213115>

\*\*\* <http://www.computing.co.uk/ctg/news/2321750/more-than-80-per-cent-of-employees-use-non-approved-saas-apps-report>

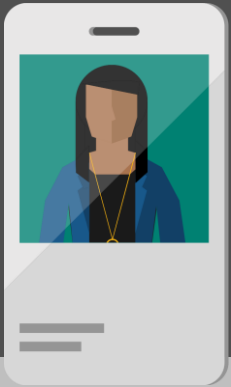
# What's Driving Change?



# Empowering Enterprise Mobility

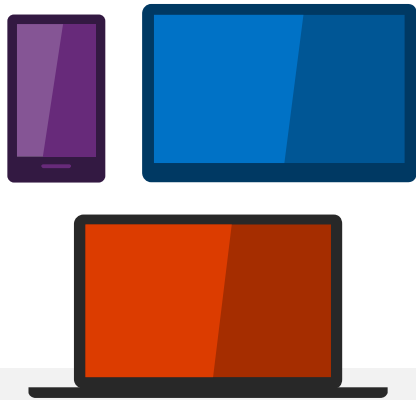
People-centric approach

User



Enable  
your users

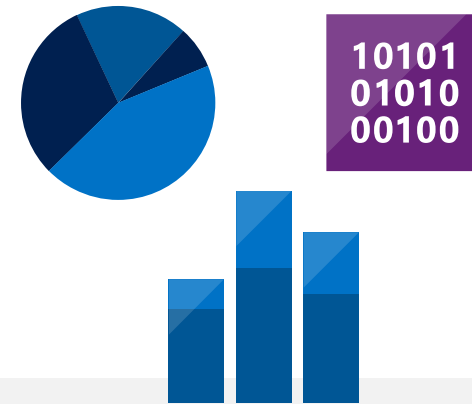
Devices



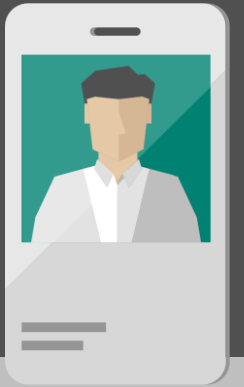
Apps



Data



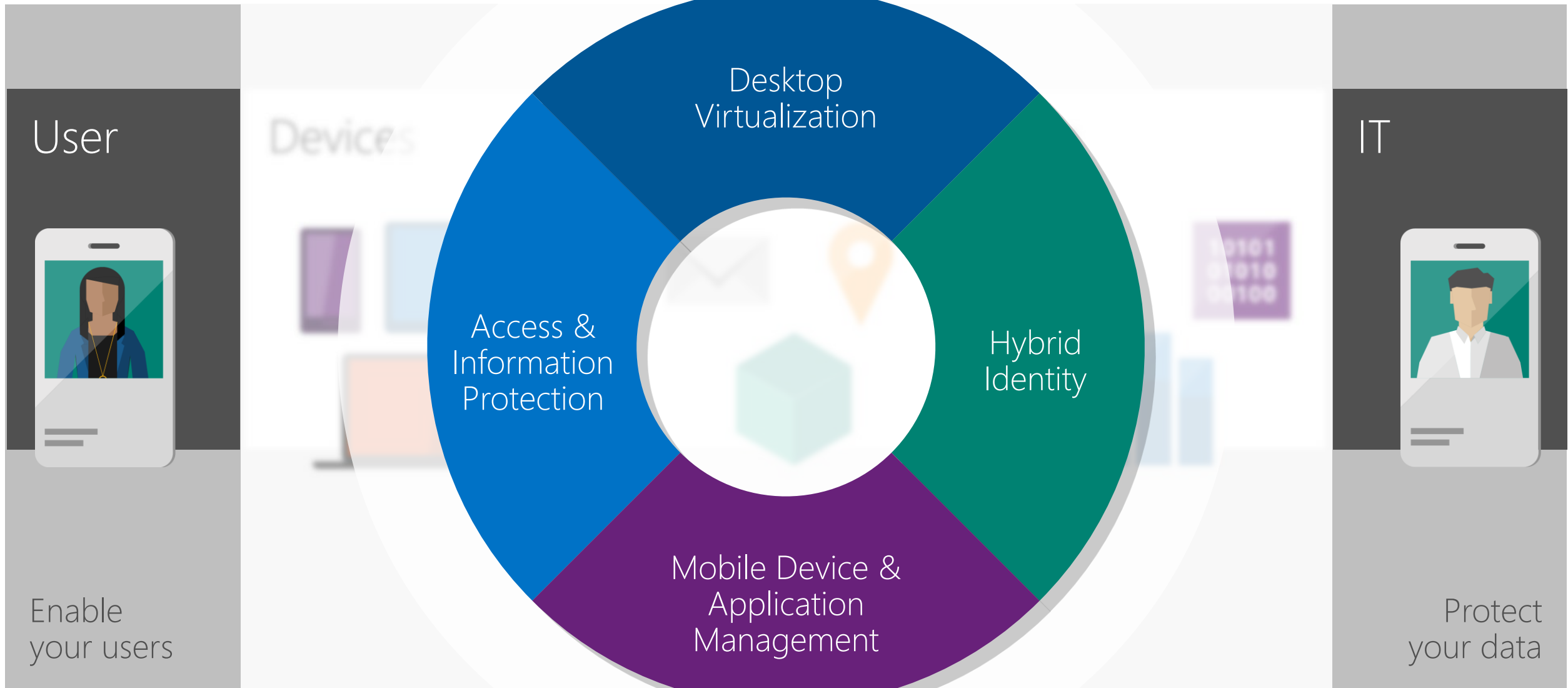
IT



Protect  
your data

Unify Your Environment

# Empowering Enterprise Mobility



# What is the Enterprise Mobility Suite?

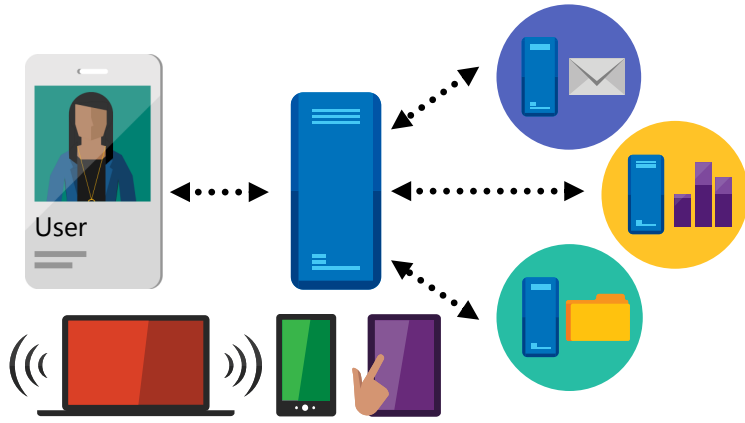
Hybrid identity	Microsoft Azure Active Directory Premium		
	security reports, and audit reports, multi-factor authentication	Self-service password reset and group management	Connection between Active Directory and Azure Active Directory
Mobile device management	Microsoft Intune		
	Mobile device settings management	Mobile application management	Selective wipe
Access & Information protection	Microsoft Azure Rights Management service		
	Information protection	Connection to on-premises assets	Bring your own key

Enterprise Agreement (EA) prices starting at \$4 per user per month

Limited time EA Level A promotion pricing. Requires 250 seat minimum purchase and underlying CAL Suite license (Core CAL Suite and Enterprise CAL Suite)



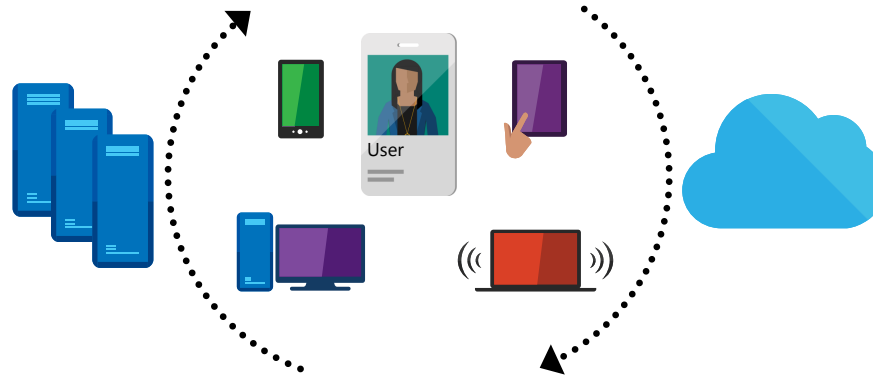
# Hybrid Identity



Enable users

## Unify your environment

Create a **centralized identity** across on-premises and cloud  
Use **identity federation** to maintain centralized authentication and securely share and collaborate with external users and businesses



Unify your environment

## Enable users

Provide users with **self-service experiences** to keep them productive  
Enable **single sign-on** for users across all the resources they need access to

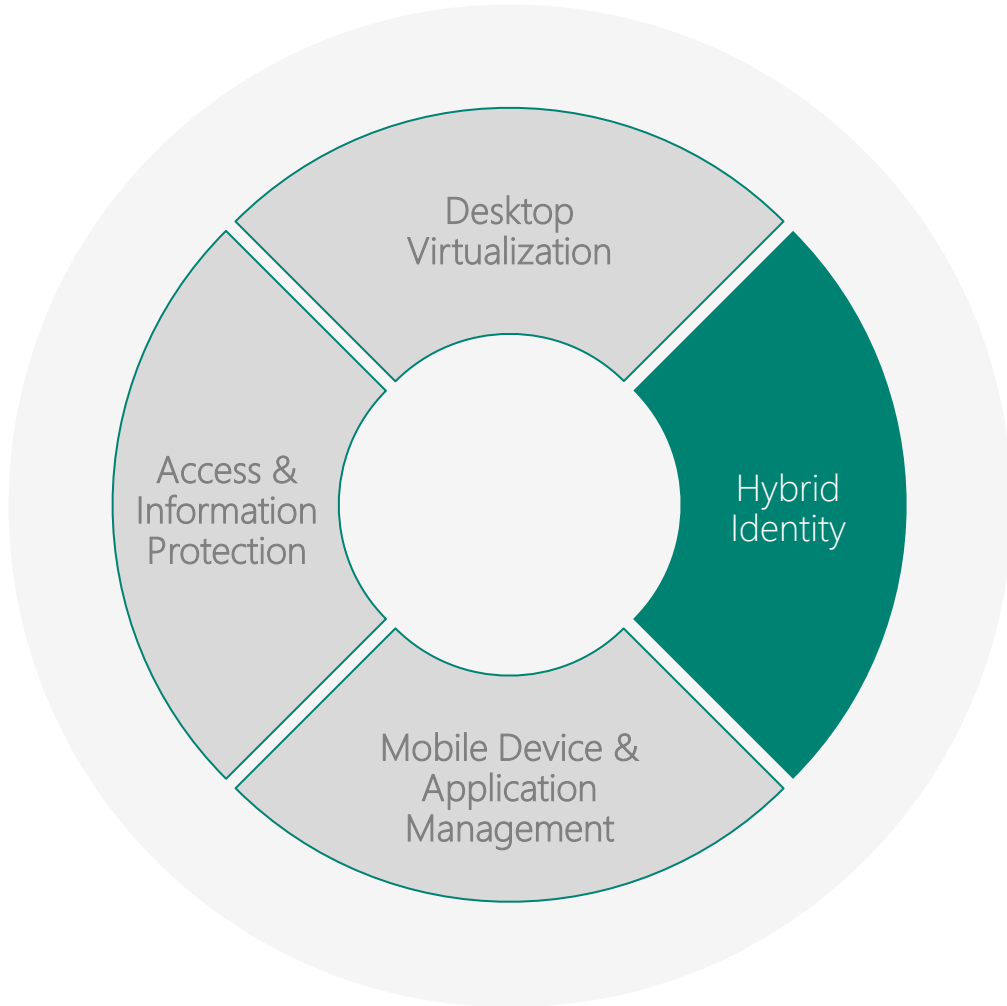


Protect your data

## Protect your data

Enforce **strong authentication** when users access resources and apply **conditional access controls** to sensitive company information  
**Configure single sign-on** across all company applications  
Ensure compliance with **governance, attestation and reporting**

# One User. One Identity. Everywhere.



- ▶ Single sign-on
- ▶ Self-service experiences
- ▶ Common identity
- ▶ Conditional access
- ▶ SaaS applications



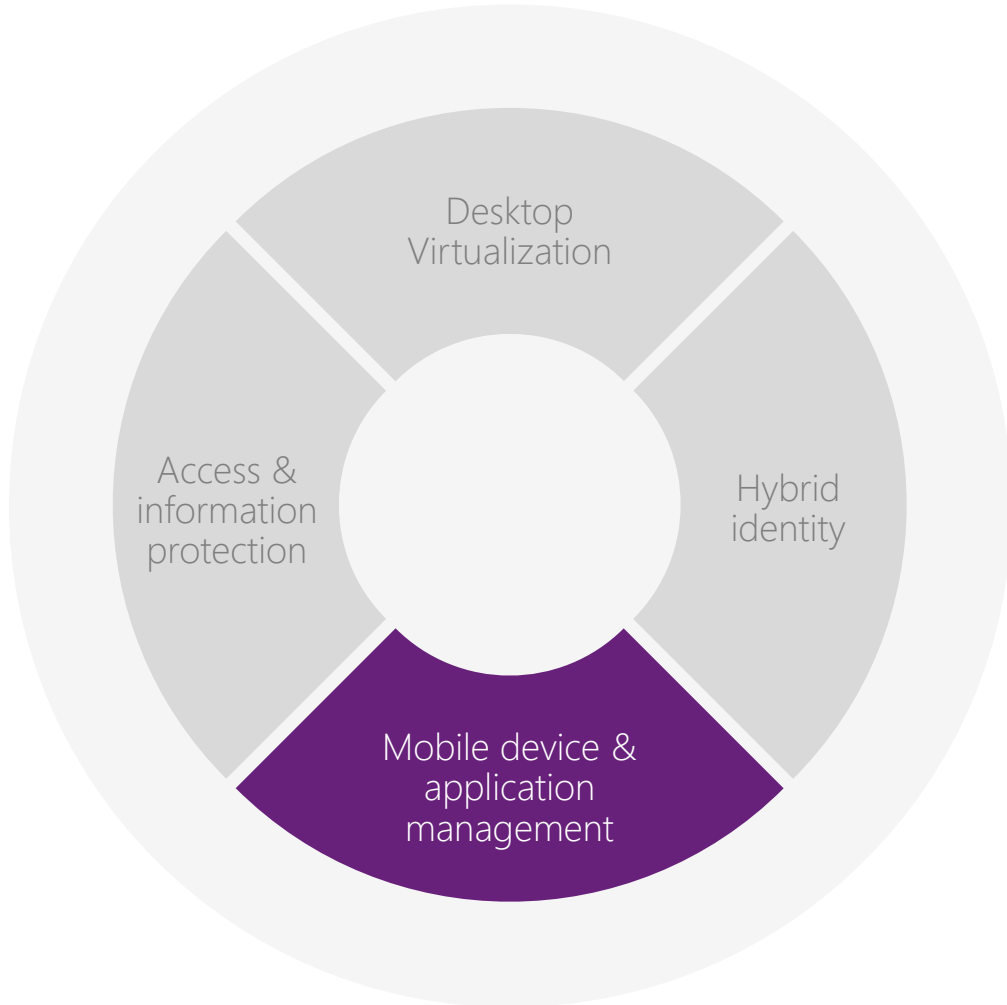
# DEMO

Conditional Access

Application Granularity – RBAC

Controlled access to SAAS Apps

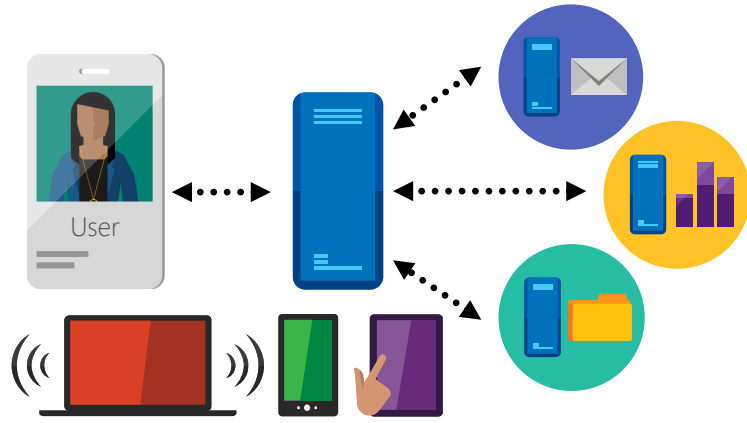
# Device choice. Simplified management.



- ▶ Consistent user experience
- ▶ Simplified device enrollment and registration
- ▶ Single console to manage devices
- ▶ Application management for Office and LOB



# User and Device Management

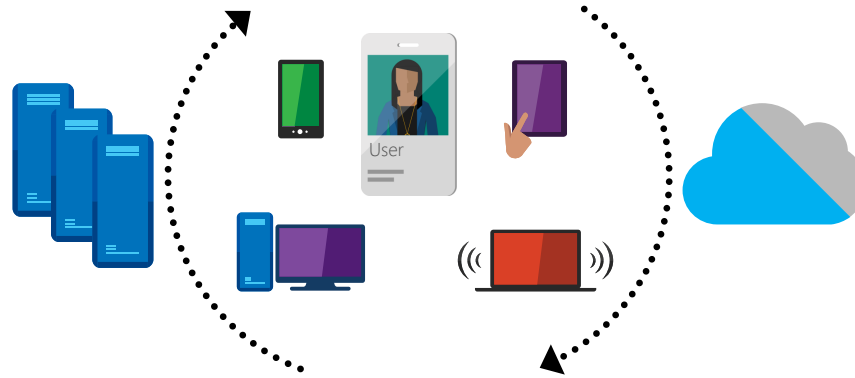


## Enable users

Access to company resources consistently across devices

Simplified registration and enrollment of devices

Synchronized corporate data



## Unify your environment

On-premises and cloud-based management of devices within a single console.

Simplified, user-centric application management across devices

Comprehensive settings management across platforms, including certificates, VPNs, and wireless network profiles



## Protect your data

Protect corporate information by selectively wiping apps and data from retired/lost devices

A common identity for accessing resources on-premises and in the cloud

Identify which mobile devices have been compromised

# Managing Office Mobile Apps with Intune



Office 365 and Intune protect data on mobile devices without sacrificing user productivity

## Secure Collaboration

- IT can set and manage policy around how data is shared with managed and non-managed apps
- In addition to Office mobile apps for iOS and Android, Intune will support management of LOB iOS and Android apps

## Rich Office Experience

- Give users familiar, full-featured Office applications
- Maintain document formatting across platforms
- Securely store, sync, and share content via OneDrive for Business

# DEMO

Unified device management with SCCM+ Intune

Application blocking

Company portal

Mobile Application management (Load, Push, Update)

# Key learnings from our customers

Data privacy is important  
and is often mandated

Regulatory requirements  
are on the rise

The perimeter is fading...

Mobile workforces, BYOD,  
outsourcing, virtual orgs

Many models of  
data protection polices  
are more reactive

We need data to be born  
encrypted and to maintain a  
persistent protection

IT must 'reason over data'  
as they do high value  
services

Point to point encryption  
fails them today

Waiting for the "ultimate  
data protection solution" is  
tempting

... yet data is leaking now

P2P federation is not  
practical or scalable

There has to be a better way



# Our approach

## **Protect any file type**

Delight with Office docs,  
PDF, Text, and Images.

## **Protect in place, and in flight**

Data is protected all the time

## **Share with anyone**

B2B sharing is most  
important with  
B2C on the rise

## **Important applications and services are enlightened**

Delight with Office docs,  
PDF, Text, and Images.

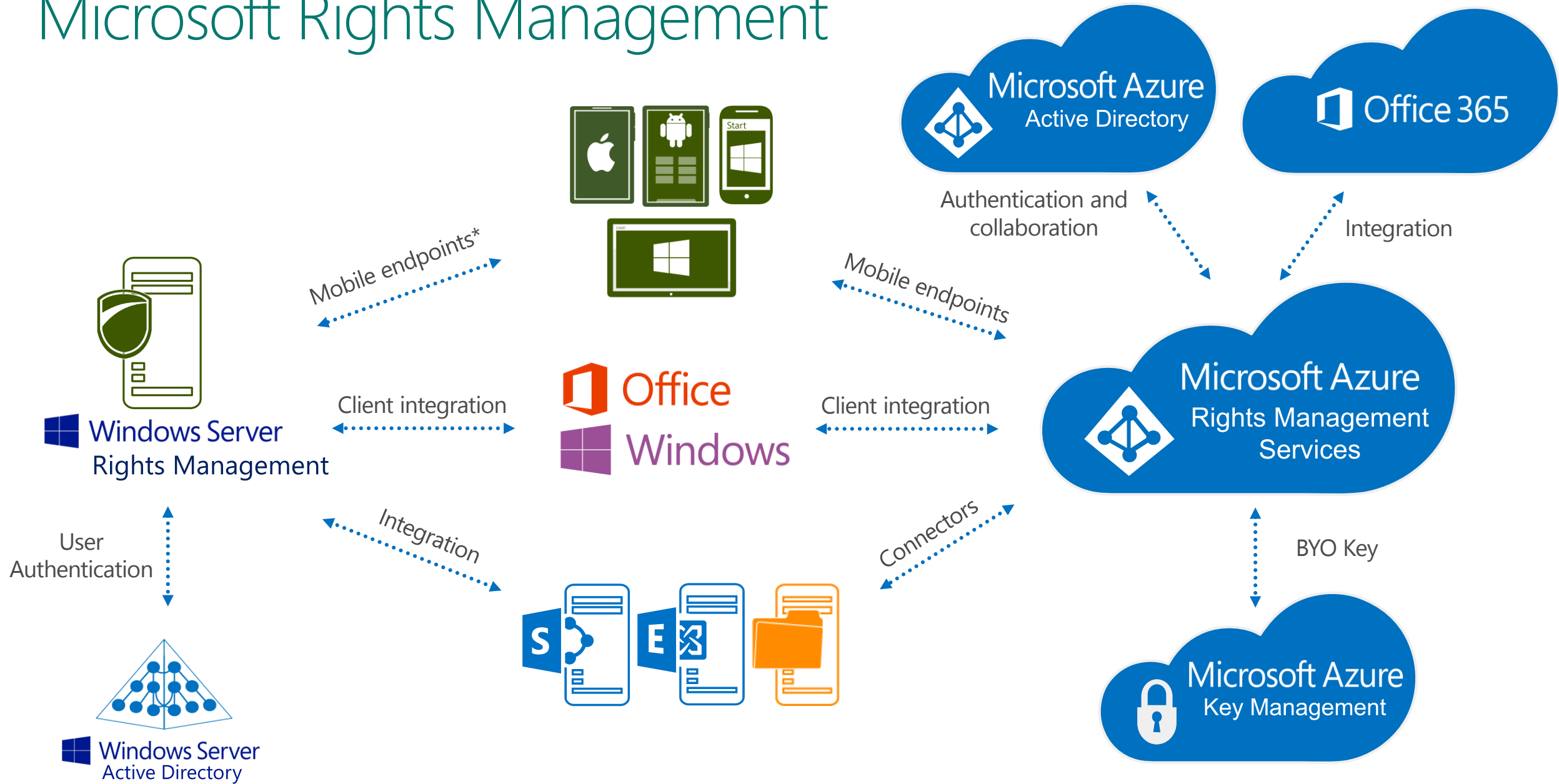
## **Meet the varied organizational needs**

Protection enforced in the  
cloud, or on-premises; with  
data in both places.

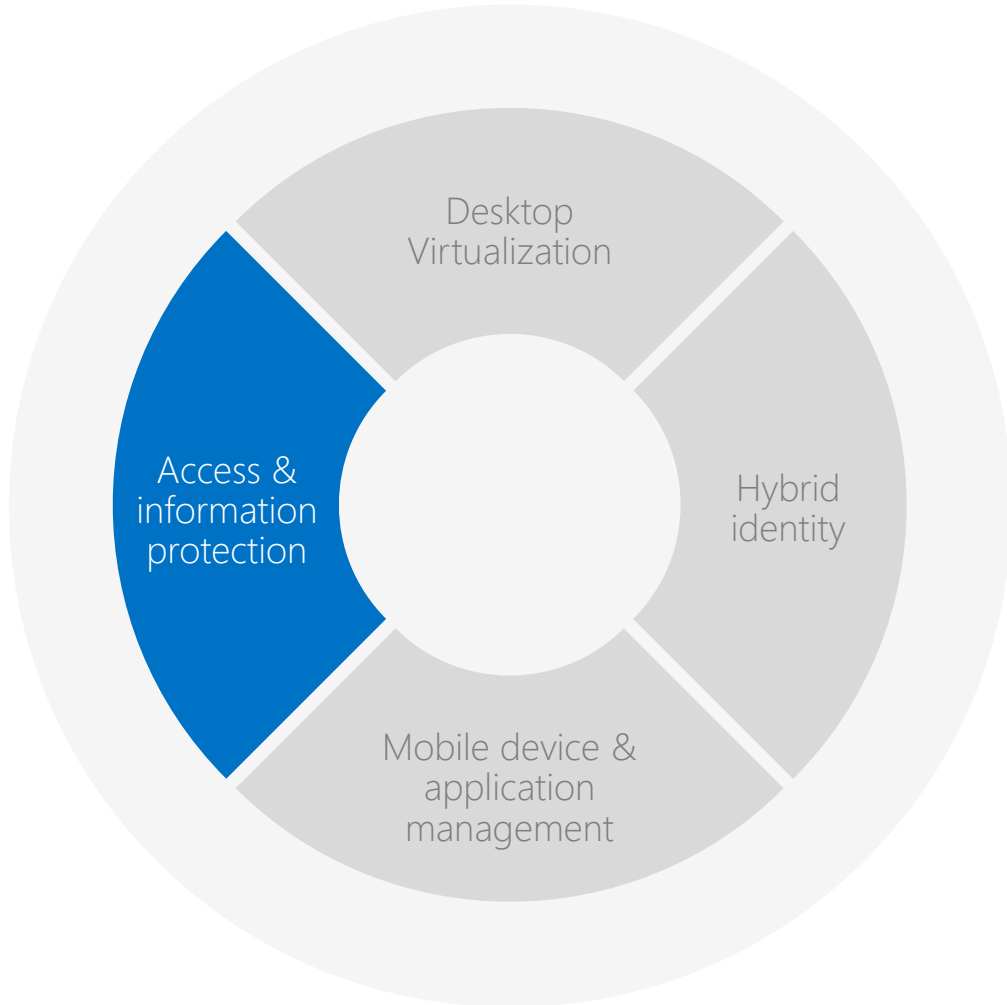
## **CSOs and Services can 'reason over data'**

Delegated access to data  
with bring-your-own-key

# Microsoft Rights Management



# Right info. Right person. Right device.



- ▶ Dynamic Access Control
- ▶ Rights management
- ▶ Secure access to work files



# DEMO

Protect in Place

Protect Shared Information

Protect in stores

SharePoint

Exchange

One Drive integration

FCI and Fileserver integration

B2B – Share protected

# Why the suite? - Comprehensive

## Other options in the market

### Cloud and hybrid identity management

*Extend corporate user identities to a variety of mobile devices and apps*

Okta      Salesforce Identity  
Ping Identity      Google  
Amazon Web Services  
Centrify

### Mobile device management

*Manage multiple device types running multiple operating systems*

AirWatch      MobileIron  
Symantec      Kaseya  
Good

### Information Protection

*Ensure robust data protection*

Adobe LiveCycle      Fasoo  
Seclore

## Why Microsoft?

- User productivity across devices
- Security and regulatory compliance
- Mobile device & app management
- Sensitive data protection

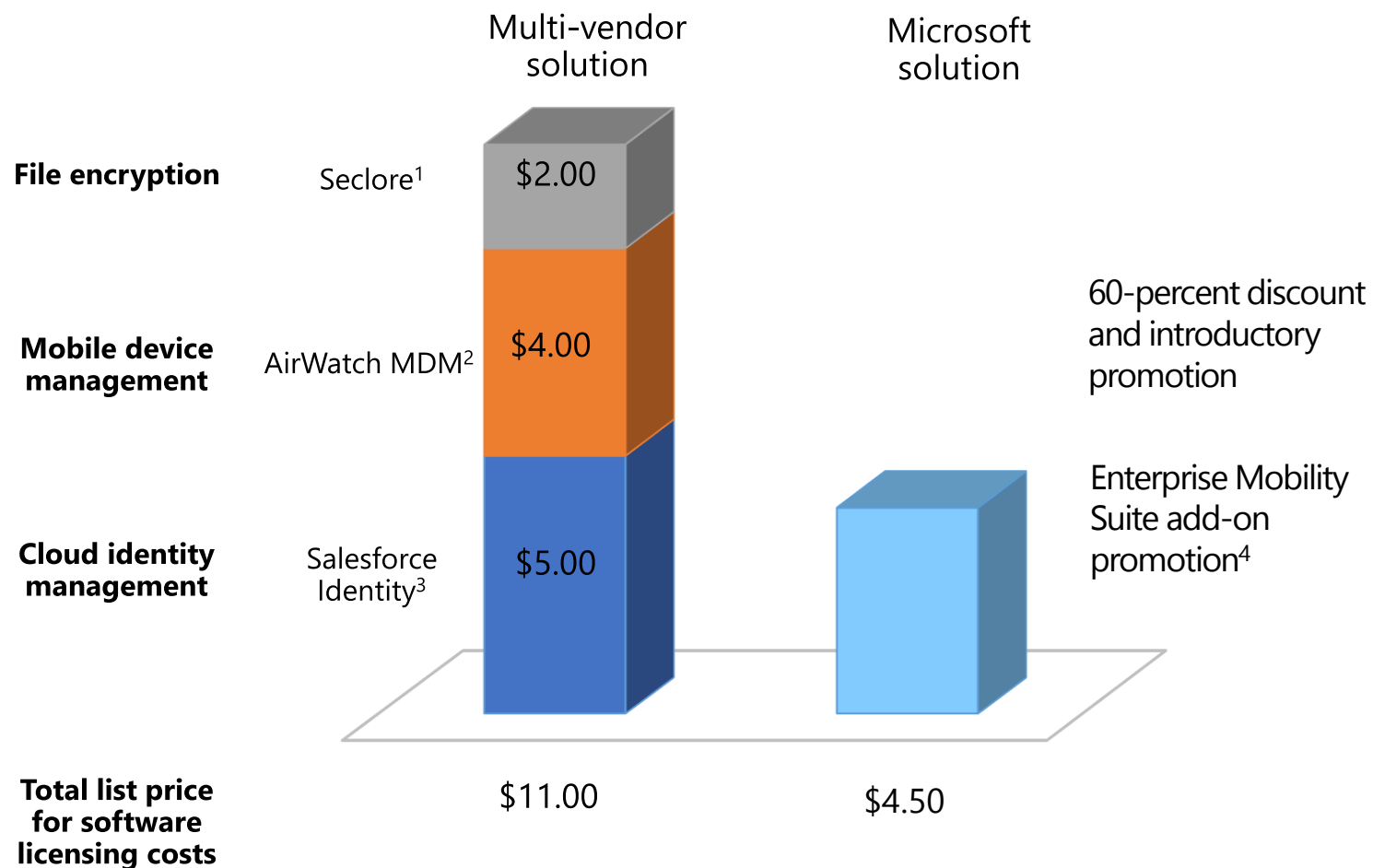
One Vendor, One Contract, One SKU

Azure Active Directory Premium

Microsoft Intune

Azure Rights Management service

# Why the Suite? - Cost Effective



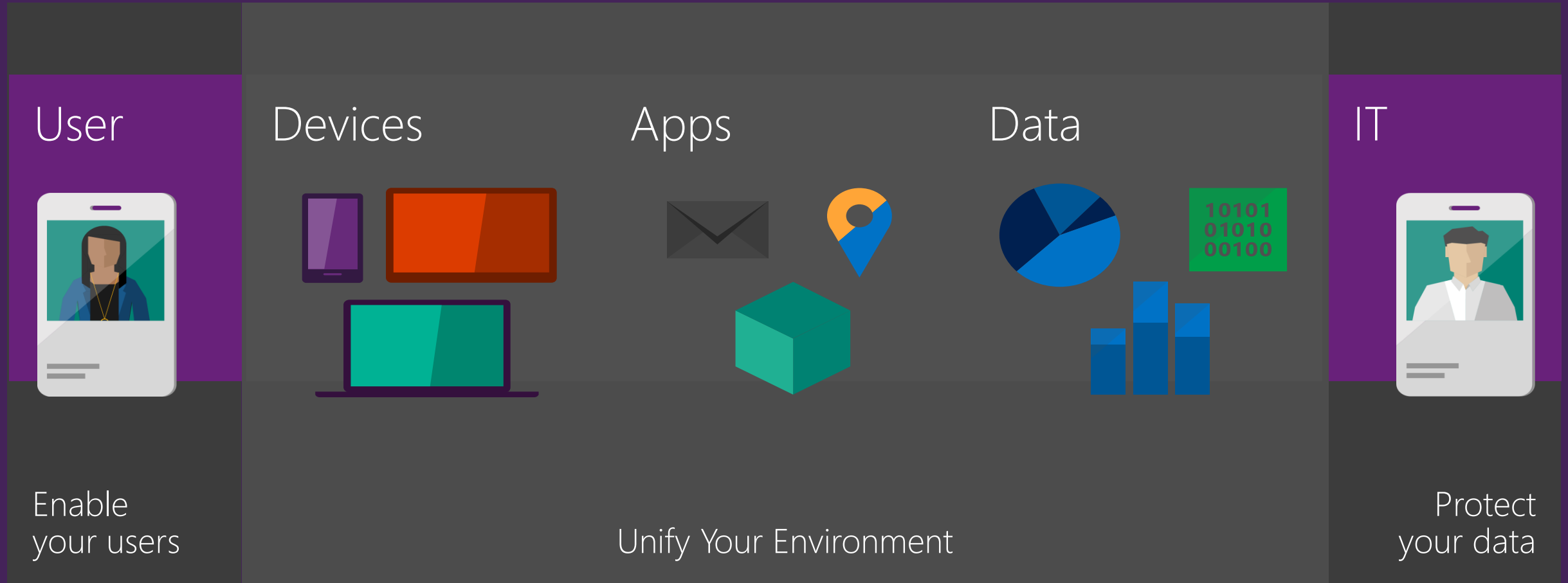
People-centric IT with one license suite and one vendor

**60-percent** discount over list pricing with limited time promotion

Add-on SKU requires Core CAL, ECAL, or Bridge CAL

1. Seclore assumes blended cost across 500 authors (\$7 per user), 1000 consumers (no cost).
2. AirWatch per device per month Cloud Hosted MDM Suite List pricing. Management of multiple devices per user requires additional licensing.
3. Salesforce Identity per user per month list pricing, included for existing Salesforce customers. Okta list price \$10 per user per month.
4. Per user per month Open NL price \$4.5/u/m. EA pricing starts at \$4/u/m. Promo requires 250 minimum purchase and qualifying CAL Suite license.

# Enterprise Mobility Vision



*Help organizations enable their users to be productive on the devices they love while helping ensure corporate assets are secure*

# Your Feedback is Important

Fill out evaluation of this session and help shape future events.

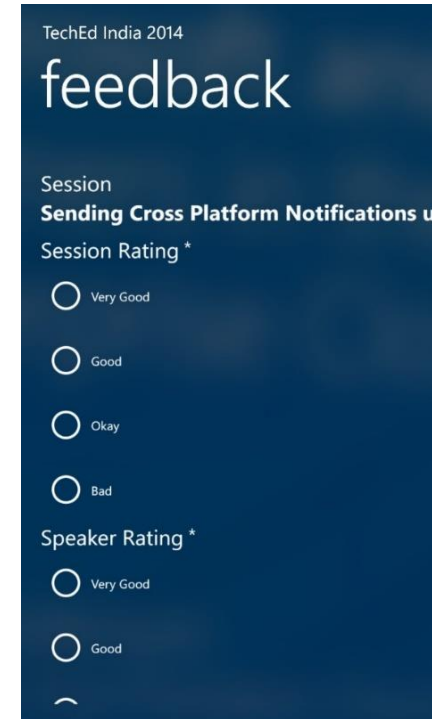


## OPTION 1



Scan the QR code to evaluate this session on your mobile device.

## OPTION 2

A screenshot of a mobile app interface for feedback. At the top, it says "TechEd India 2014" and "feedback". Below that, it says "Session Sending Cross Platform Notifications us". Then "Session Rating \*" with four radio button options: "Very Good", "Good", "Okay", and "Bad". Below that, it says "Speaker Rating \*" with two radio button options: "Very Good" and "Good". At the bottom, there is a back arrow icon.

You can fill out evaluation of this session directly through the App

OPTION 3: Feedback stations outside the hall





© 2014 Microsoft Corporation. All rights reserved. Microsoft, Windows, and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries. The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.

# What's the EMS benefit for O365 customers?

## Desktop EA

Domain-based identity management  
(single sign-on for on-premises applications)

Centralized PC management

Information protection for on-premises  
Office deployments

On-premises solution

## Desktop EA + Office 365

Hybrid identity and single sign-on for  
Office 365

Multi-factor authentication for Office 365

Cloud-based information protection for  
Office 365

Mobile Device settings management

Cloud solution

## Enterprise Mobility Suite

security reports, and multi-factor  
authentication

Self-service password reset and Group  
management

Connection between Active Directory and  
Azure Active Directory

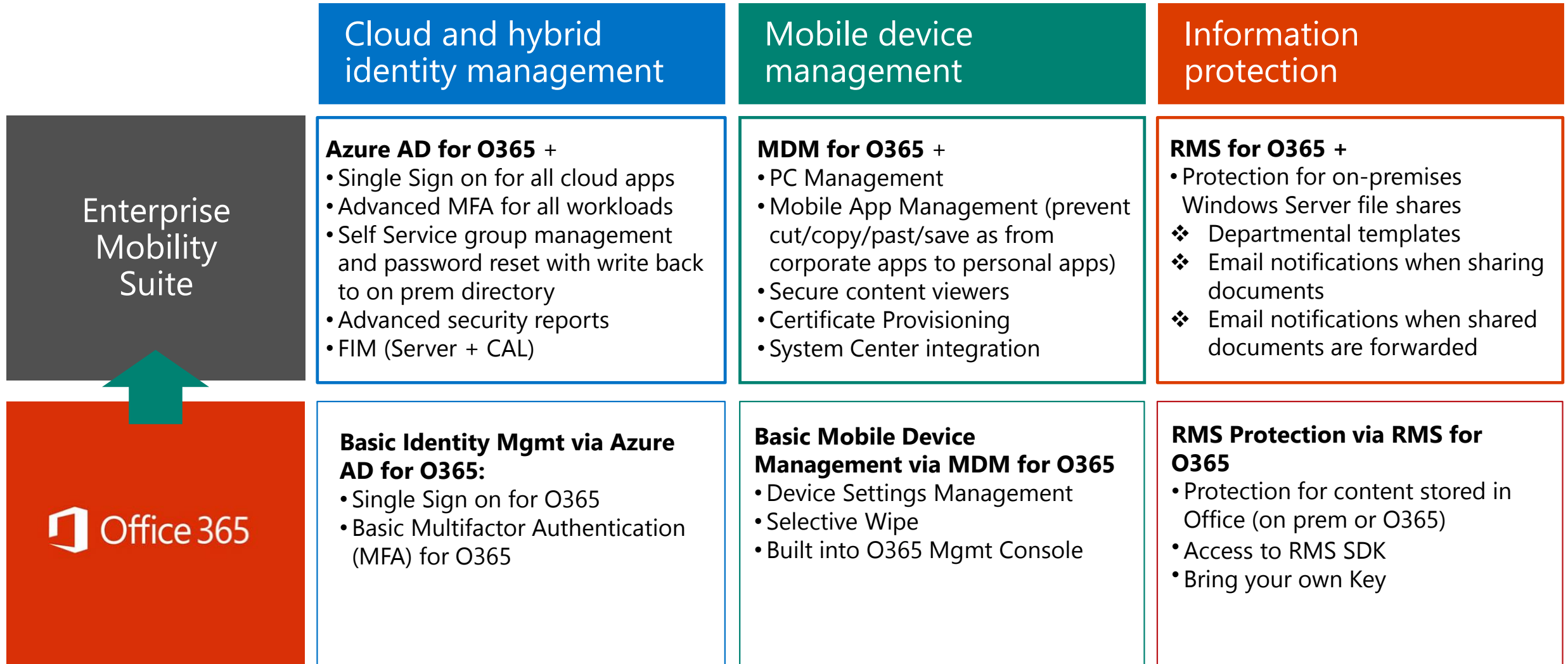
Mobile application management

Selective wipe

Information protection

Connection to on-premises assets

# EMS IT Manageability benefits for O365 customers



# Azure Active Directory Offering Comparison

	Azure AD Free (O365)	Azure AD Premium
Directory as a service	✔ Up to 500,000 objects	✔ No limit
User and group management	✔	✔
Single sign-on for pre-integrated SaaS and custom applications	✔ 10 apps per user	✔ No limit
Microsoft Directory Synchronization Tool (Windows Server Active Directory extension)	✔	✔
User-based access management and provisioning	✔	✔
Group-based access management and provisioning		✔
Self-service group management for cloud users		✔
Self-service password change for cloud users	✔	✔
Self-service password reset for cloud users		✔
Security reports	✔	✔
Advanced security reporting (based on machine learning)		✔
Usage reporting		✔
Company branding (logon pages and Access Panel customization)		✔
Multi-factor authentication (all available features on Windows Azure and on-premises environments)		✔
Service-level agreement (SLA)		✔
Forefront Identity Manager CAL + Forefront Identity Manager Server		✔

# Azure MFA Offering Comparison

	MFA for O365/Azure Administrators	Windows Azure Multi-Factor Authentication / EMS
Administrators can Enable/Enforce MFA to end-users	✓	✓
Use Mobile app (online and OTP) as second authentication factor	✓	✓
Use Phone call as second authentication factor	✓	✓
Use SMS as second authentication factor	✓	✓
Application passwords for non-browser clients (e.g. Outlook, Lync)	✓	✓
Default Microsoft greetings during authentication phone calls	✓	✓
Custom greetings during authentication phone calls		✓
Fraud alert		✓
MFA SDK		✓
Security Reports		✓
MFA for on-premises applications/ MFA Server.		✓
One-Time Bypass		✓
Block/Unblock Users		✓
Customizable caller ID for authentication phone calls		✓
Event Confirmation		✓

# Azure RMS Offering Comparison

	RMS for O365	Azure RMS (EMS)
Consume & Create RMS content with company ID	✓	✓
Protection for content stored in O365	✓	✓
Protection for content stored in on prem Office (Exchange, Sharepoint via RMS Connector)	✓	✓
Bring your own Key (Hybrid protection)	✓	✓
RMS protection for non office files	✓	✓
RMS SDK	✓	✓
RMS On Prem Connector for on-premises Windows Server file shares* (via RMS FCI Connector)		✓

\* As of July 1, 2014

# Device management feature comparison

Category	Feature	Exchange ActiveSync	MDM for Office 365	Intune
Device configuration	Inventory mobile devices that access corporate applications	✓	✓	✓
	Remote factory reset (full device wipe)	✓	✓	✓
	Mobile device configuration settings (PIN length, PIN required, lock time, etc.)	✓	✓	✓
	Self-service password reset (Office 365 cloud only users)	✓	✓	✓
Office 365	Provides reporting on devices that do not meet IT policy		✓	✓
	Group-based policies and reporting (ability to use groups for targeted device configuration)		✓	✓
	Root cert and jailbreak detection		✓	✓
	Remove Office 365 app data from mobile devices while leaving personal data and apps intact (Selective wipe)		✓	✓
	Prevent access to corporate email and documents based upon device enrollment and compliance policies		✓	✓
Premium mobile device & app management	Self-service Company Portal for users to enroll their own devices and install corporate apps			✓
	Deploy certificates, VPN profiles (including app-specific profiles), and Wi-Fi profiles			✓
	Prevent cut/copy/paste/save as of data from corporate apps to personal apps (Mobile application management)			✓
	Secure content viewing via Managed browser, PDF viewer, Imager viewer, and AV player apps for Intune			✓
	Remote device lock via self-service Company Portal and via admin console			✓
PC management	PC management (e.g. inventory, antimalware, patch, policies, etc.)			✓
	OS deployment (via System Center ConfigMgr)			✓
	PC software management			✓
	Single management console for PCs and mobile devices (through integration with System Center ConfigMgr)			✓