

Endpoint Management Workshop

Unified endpoint management to secure the modern workplace

Tracy Wetherington

Yorktel
Modern Workplace



Technology needs are evolving in the modern workplace

Fragmented



Integrated

Closed Perimeter



Cloud

Less Regulated



More Regulated

Manual



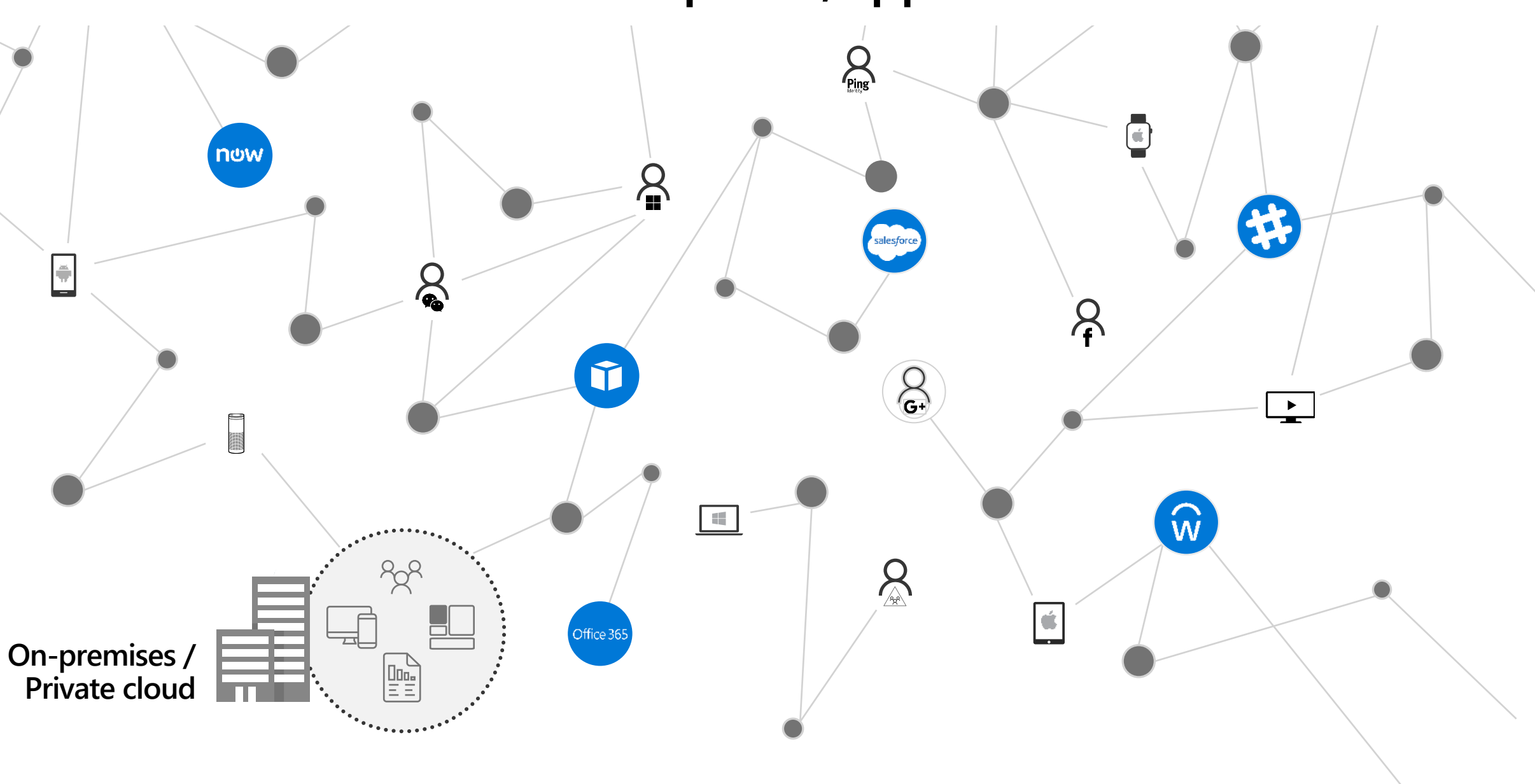
Automated

Insourced



Managed

Proliferation of endpoints, apps and threats



IT challenges of the modern workplace

How do you empower users while protecting your most important assets?

Employee goals

Collaborate

Easy access

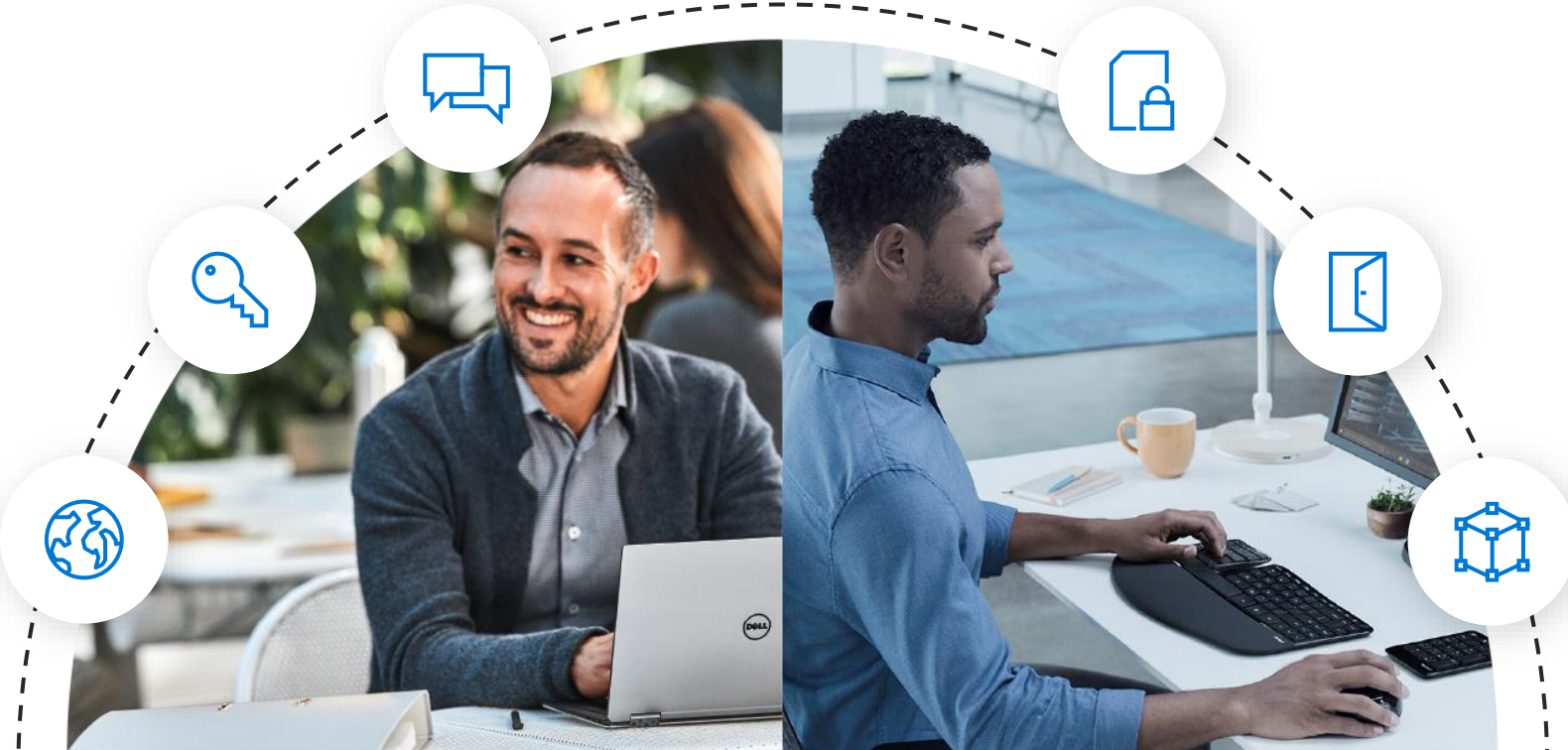
Work anywhere

IT goals

Protect data

Manage access

Stay innovative

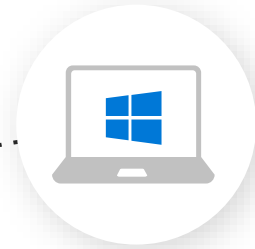


Transformative device management and security

Microsoft Flexible Device Management

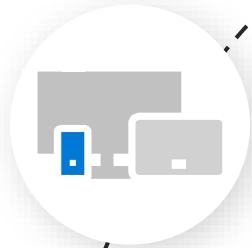


**Enable
your users**

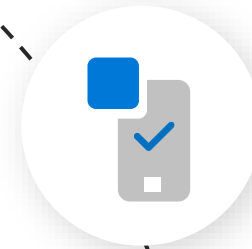


PC desktop
management

**Protect
your data**



Mobile device
management



Mobile application
management

Microsoft Endpoint Configuration Manager and Microsoft Intune



Most complete



Most secure



Fastest time to value

Why choose Microsoft?



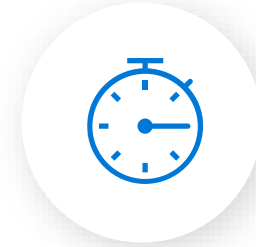
Most complete

Transform how you manage iOS, Android, macOS, and Windows devices, powered by the Microsoft intelligent cloud



Most secure

Apply conditional access and security controls for all apps and data, on corporate and personal devices



Fastest time to value

Maximize user productivity with fast roll-out of new services and out-of-box integration with Microsoft architecture and apps

Transform IT delivery and device management

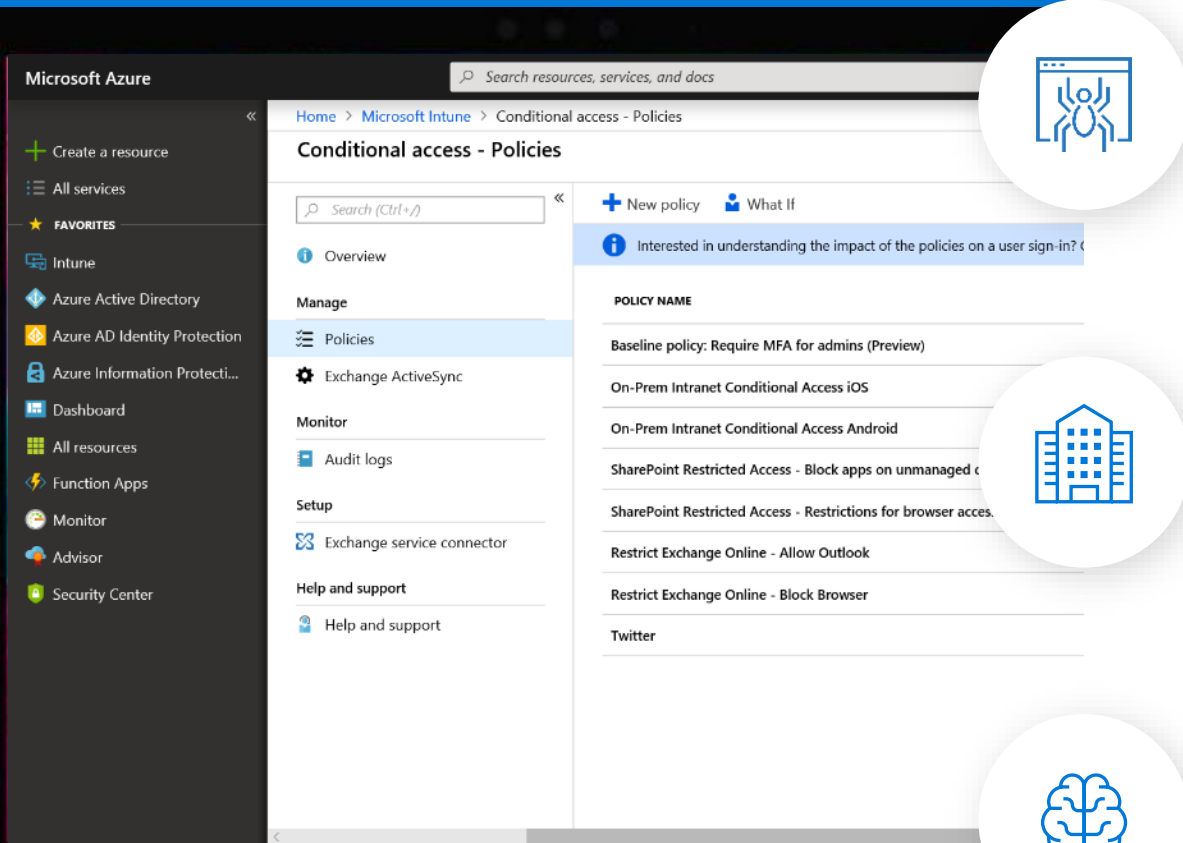
Zero-touch IT provisioning for all devices using Windows Autopilot, Apple Business Manager, or Android Enterprise

App lifecycle management for in-house (LOB) apps, public store apps, and traditional Win32 apps

Depth of **configuration and security controls** across any device



Secure apps and data in the modern workplace



Respond to internal and external threats with **real-time risk-analysis** before access to company data

Protect corporate data before, during and after they are shared, even outside the company

Extensive **visibility and intelligent cloud-powered insights** to improve end-to-end security posture

Maximize user productivity

Deliver native **app experiences** that work and feel natural on any platform

Simplify **access to resources** employees need with single sign-on, for faster service roll-out

Enable Microsoft 365 apps that users love on mobile devices, without compromising data security



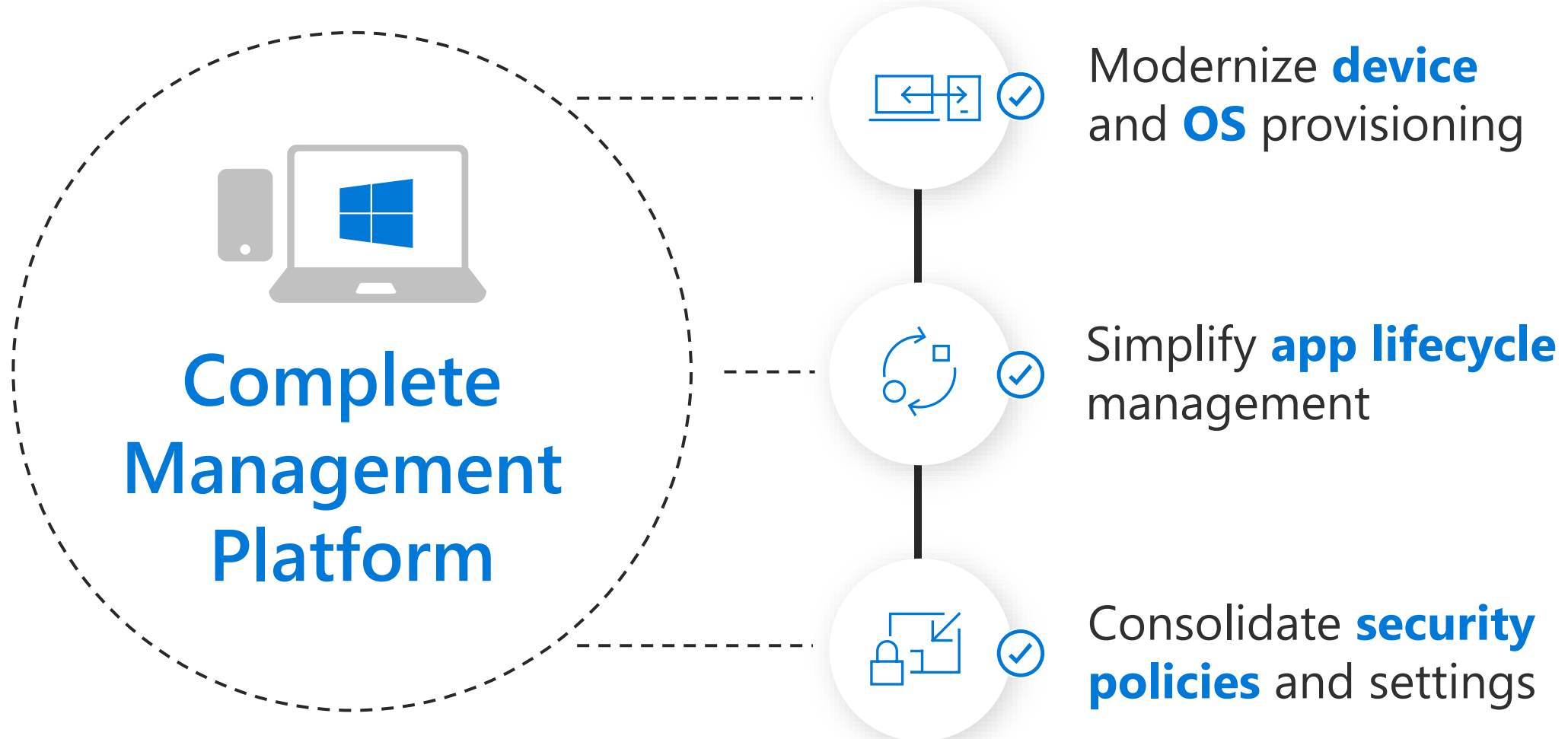


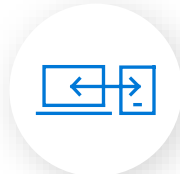
Transform Device Management

Most complete

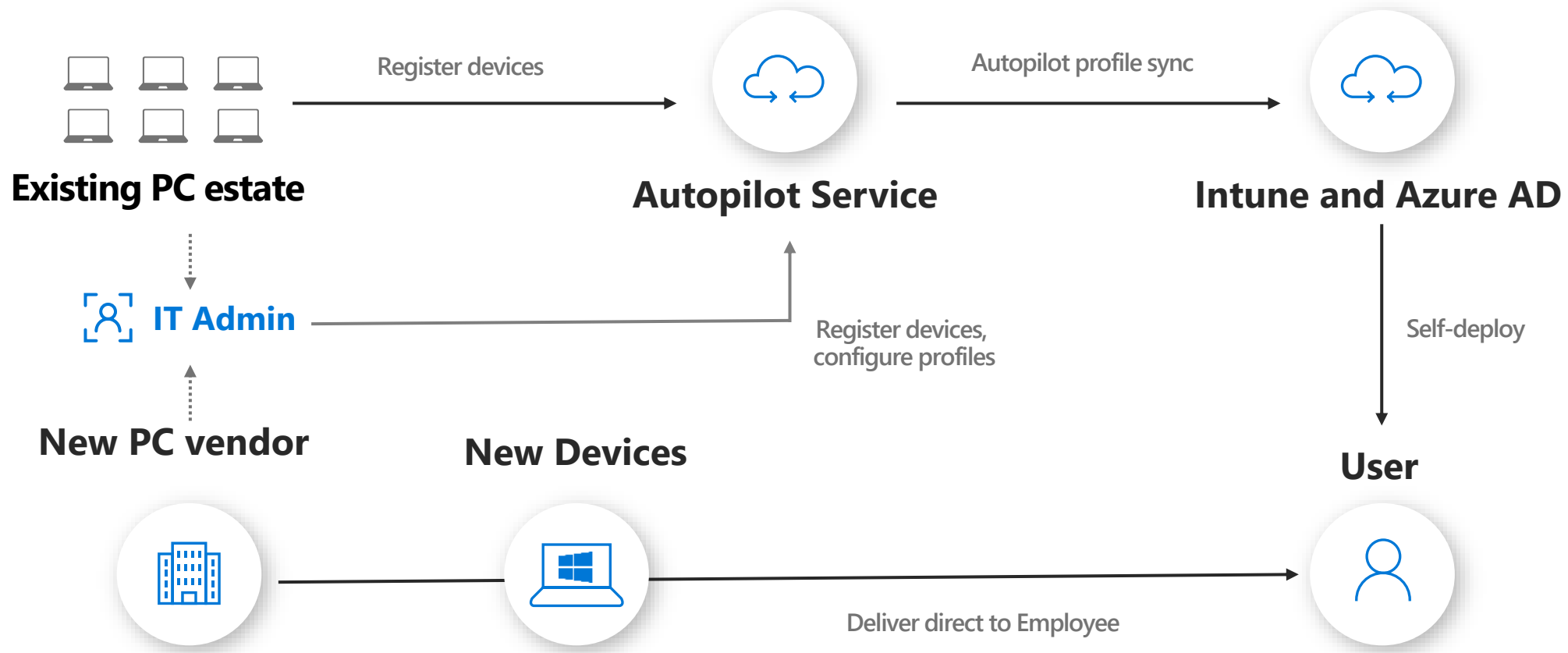


Microsoft simplifies mobile and PC management





Modern desktop provisioning with Windows Autopilot



✓ Provision new devices direct to employees, ready for use

✓ Upgrade existing devices, reimaged with Autopilot

✓ Lower IT effort and cost; user gets productive faster

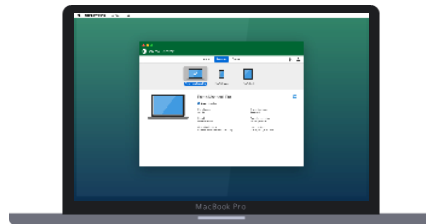


Modern device provisioning for iOS, macOS, Android



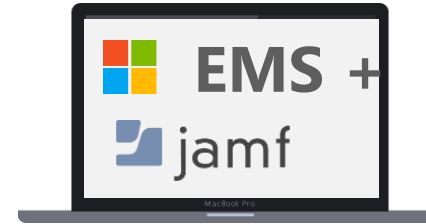
Apple iOS

Automated Device Enrollment
Apple School Manager
Apple Business Manager
Supervised Mode
Intune APP managed



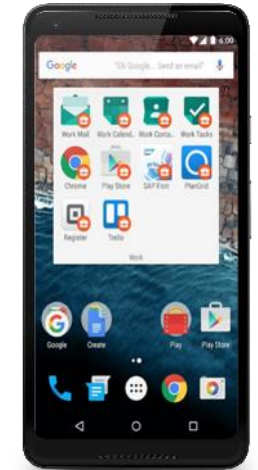
macOS

Deploying cert and settings
Zero-touch (ADE)
Conditional access
Device wipe, encryption



macOS (with Jamf)

Intune MDM features +
Extensive inventory
Scripting support
Depth of security controls
Self-service controls

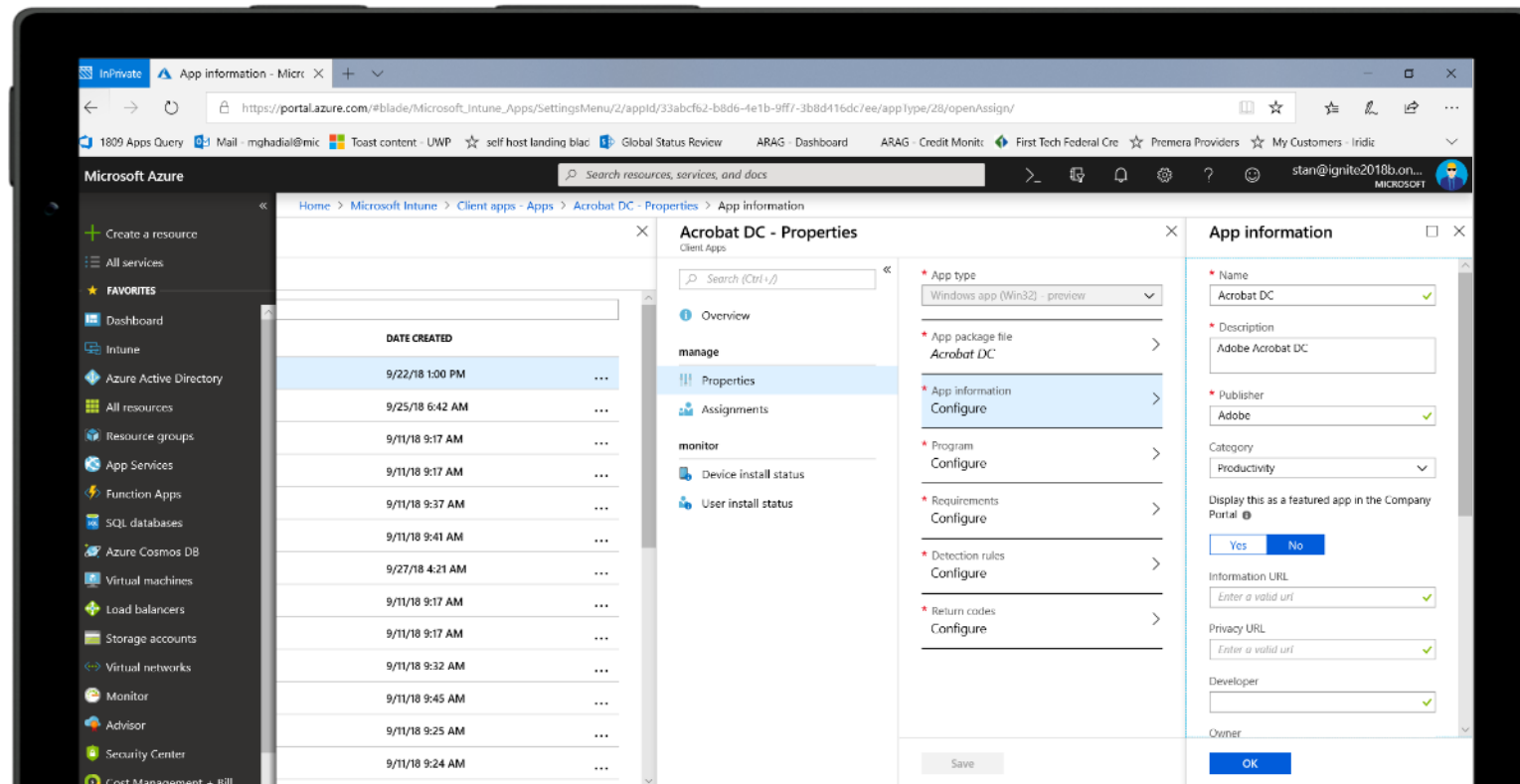


Android

Android Enterprise (ZTE)
Samsung Knox (KME)
Kiosk mode
Work Profiles
Intune APP managed



Simplify Windows application lifecycle management



Deploy Win32 apps, line-of-business (LOB) apps, and Microsoft store apps from the cloud



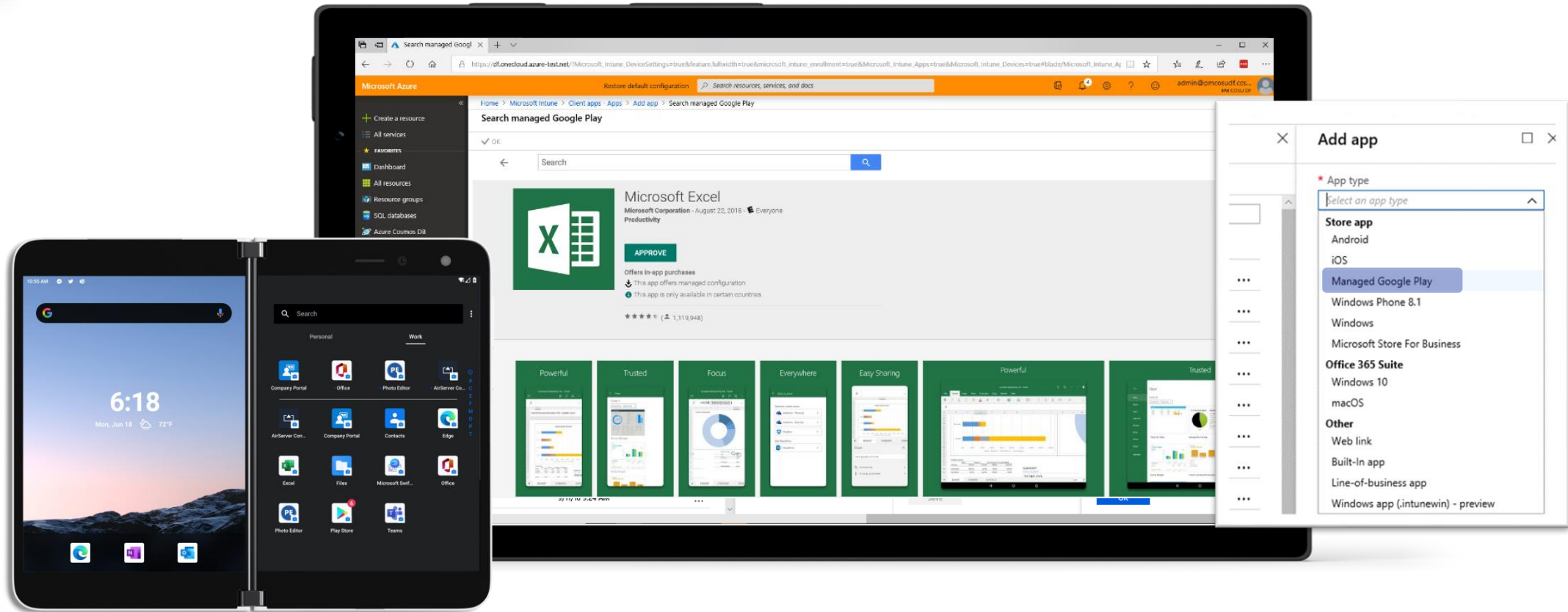
Application compatibility assurance using desktop analytics



Intune leverages Windows 10 cloud management capabilities



Simplify Managed Google Play store integration



IT control over what apps end users can install in work context



Managed app configuration; including silent installs for 'required' apps



Consistent end user experience for LoB (in-house) and Store apps; app badging in Work Profile



Simplify managed app lifecycle for iOS and macOS

The screenshot displays the 'iOS Device Management' interface. At the top, there's a navigation bar with 'Overview', 'MDM Push Certificate', 'DEP Tokens', and 'VPP Tokens'. Below this, a message states: 'You need to set up some connections between Intune and your Apple accounts before you can manage apps and settings on your iOS devices.' Three main setup cards are visible, each with a 'Manage' button and a 'Configured' status:

- Set up MDM Push Certificate** (REQUIRED BEFORE ENROLLING DEVICES): This sets up a link between your Intune account and school Apple ID so Intune can talk to your iOS devices.
- Set up Device Enrollment Program (DEP) token** (REQUIRED BEFORE ENROLLING DEVICES): You will give us some information about your school's Apple Device Enrollment Program, so Intune knows about iOS devices that you want to manage.
- Set up Volume Purchase Program (VPP) token** (OPTIONAL): If you give us some information about your Apple Volume Purchase Program, then Intune can know about your purchased iOS apps and install them on your devices.

An 'Add app' dialog box is overlaid on the right, showing a dropdown for 'App type' with the following options:

- Store app
 - Android
 - iOS
 - Windows Phone 8.1
 - Windows
- Office 365 Suite
 - Windows 10
- macOS
- Other
 - Web link
 - Built-In app
 - Line-of-business app



Distribute purchased apps from the app store (VPP) to iOS/iPadOS and macOS devices



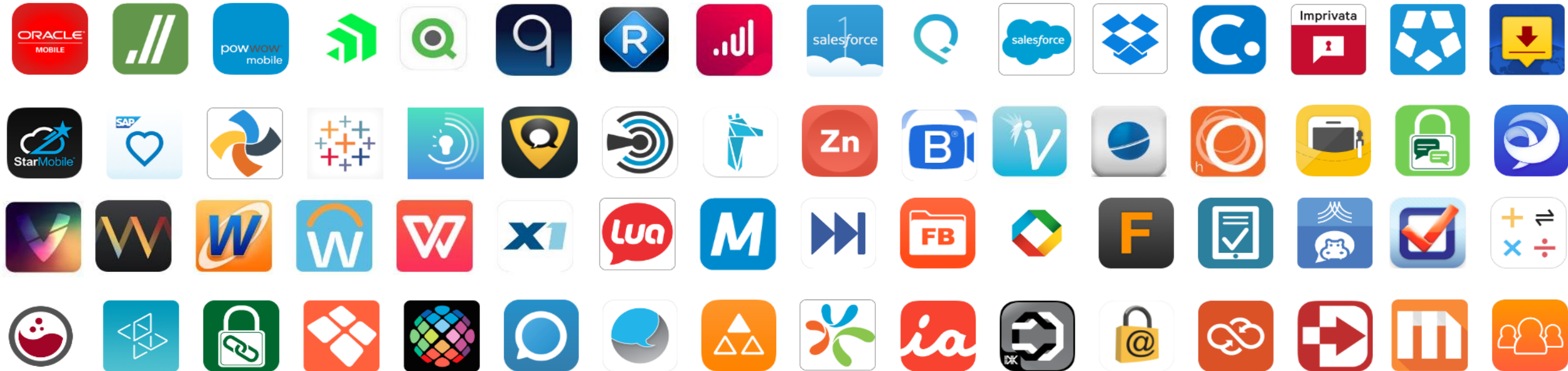
Revoke assigned VPP licenses for target app, device, or token



Simplified setup with Apple Business Manager or Apple School Manager



On managed devices, Intune can manage hundreds of 3rd party apps





Most Trusted Workplace

Most secure

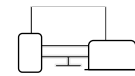
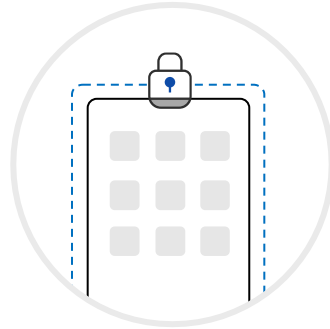


Protect your data on virtually any device with Intune

Mobile Device Management (MDM)

Conditional Access:

Restrict access to managed and compliant devices



Enroll devices for management



Provision settings, certs, profiles



Report & measure device compliance

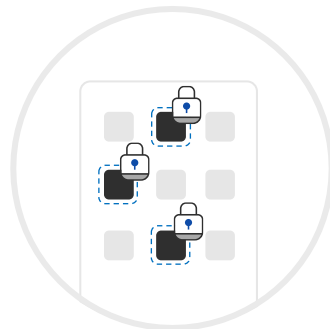


Remove corporate data from devices

Mobile Application Management (MAM)

Conditional Access:

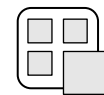
Restrict which apps can be used to access email or files



Publish mobile apps to users



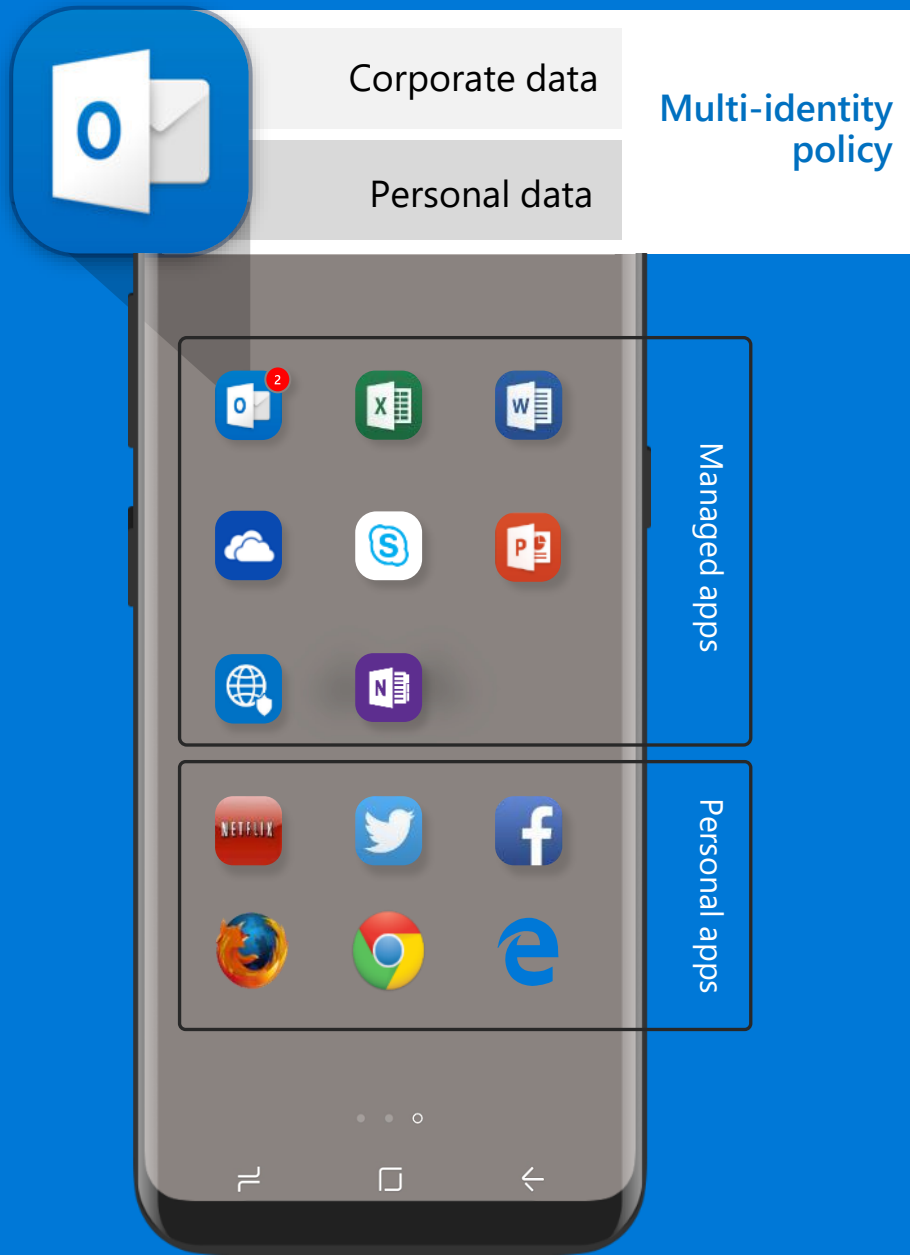
Configure and update apps



Report app inventory & usage



Secure & remove corporate data within mobile apps



App protection policies for personal devices

Enables **bring-your-own** (BYO) and personal devices at work where users may be reluctant to “enroll” their device

Ensures **corporate data cannot be copied** and pasted to personal apps within the device

Intune App Protection policies are useful to protect Microsoft 365 apps where devices are unmanaged or managed by 3rd party

Intune-enlightened apps
provide the best control, with
or without enrollment.



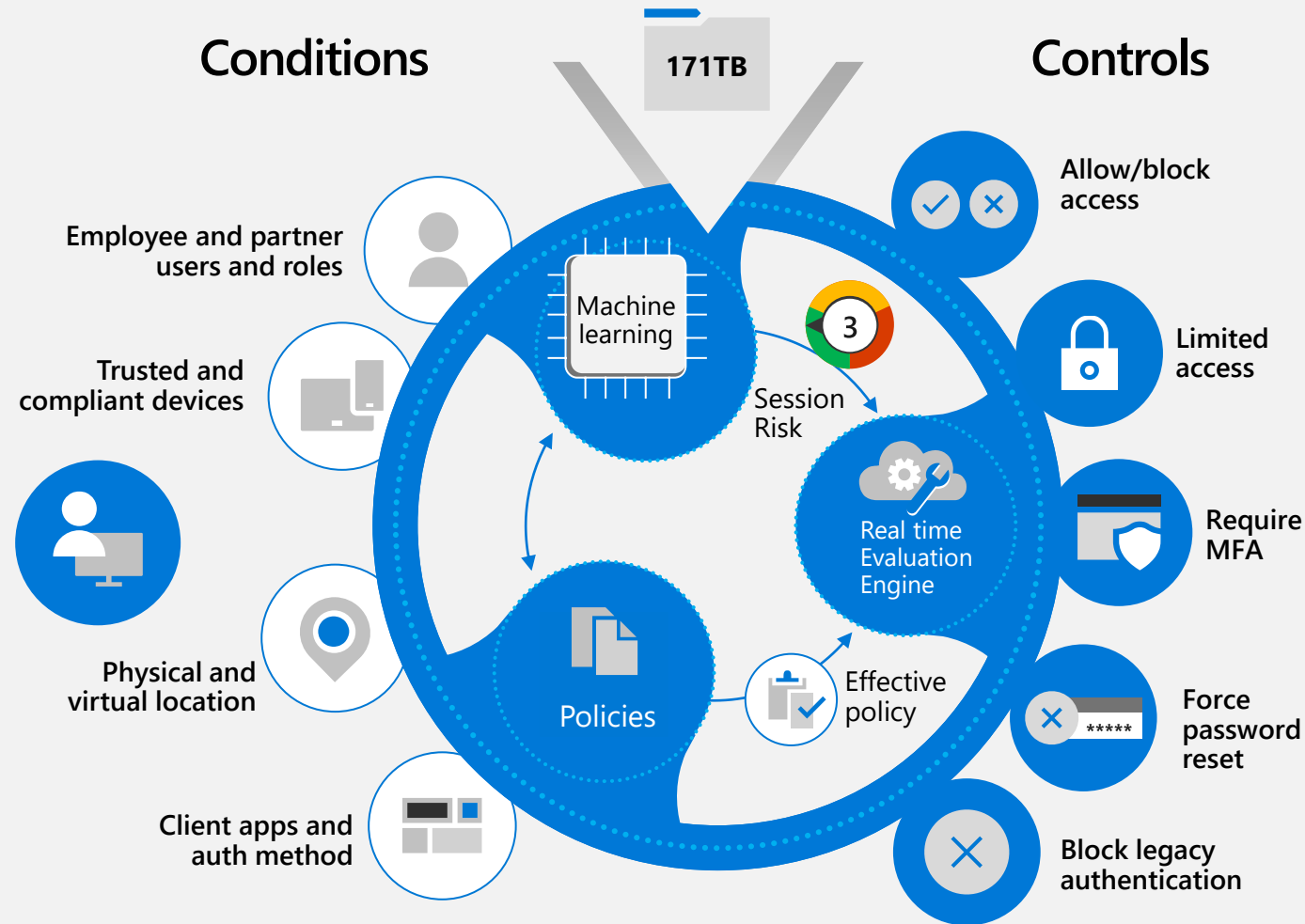
Check back frequently...
we are constantly adding new apps to this list

Conditional access to data with real-time risk analysis

Define **contextual policies** at the user, location, device, and app levels

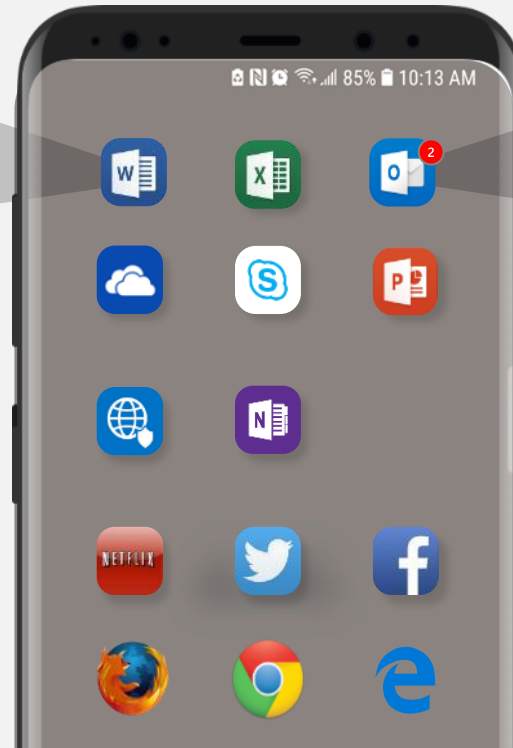
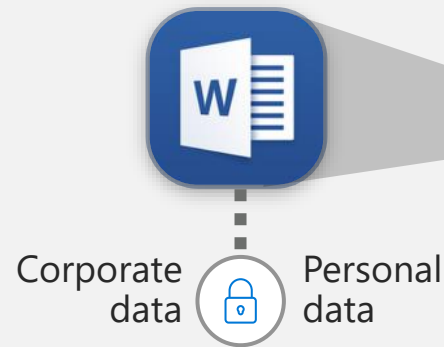
Controls adapt to **real time conditions** based on monitoring of perceived risks

Risks calculated based on **advanced Microsoft machine learning**

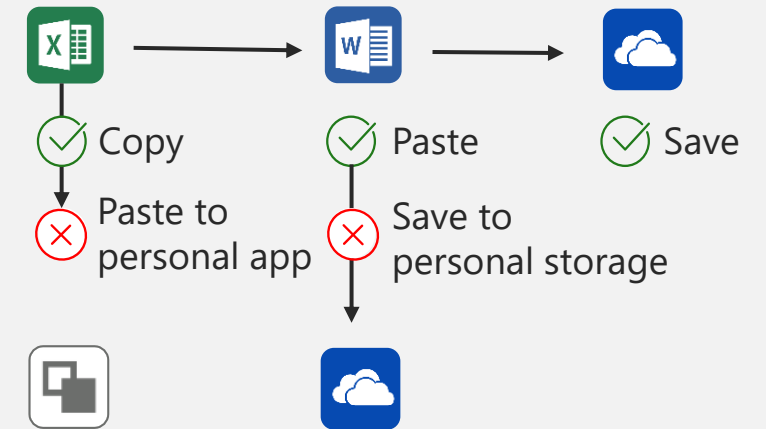


Control what happens after data has been accessed

Multi-identity policy



Email attachment

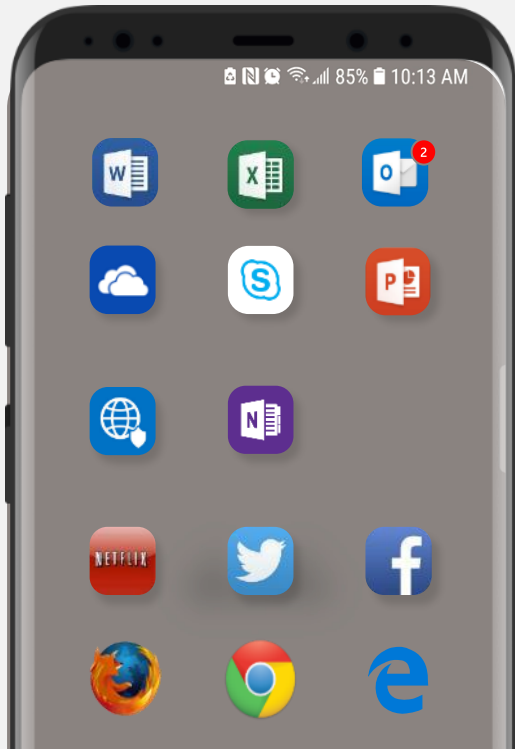


Microsoft Information Protection (MIP) empowers you to **control how data is accessed** from employee devices

Separate company managed apps from personal apps, and set policies on how data is accessed from managed apps

Intune APP **ensure corporate data can't be copied** and pasted to personal apps within the device

Intune threat protection for device risk-based conditional access

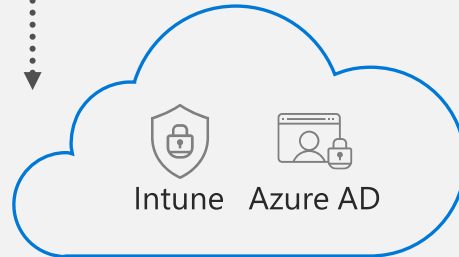


Threat protection partner detects:

- ✓ Malicious Apps
- ✓ Device manipulation
- ✓ Network exploits
- ✓ Data privacy violations

EMS role:

Intune evaluates compliance
Azure AD enforces Conditional Access



Allow
Enforce MFA
Enroll device



Block access
Wipe device

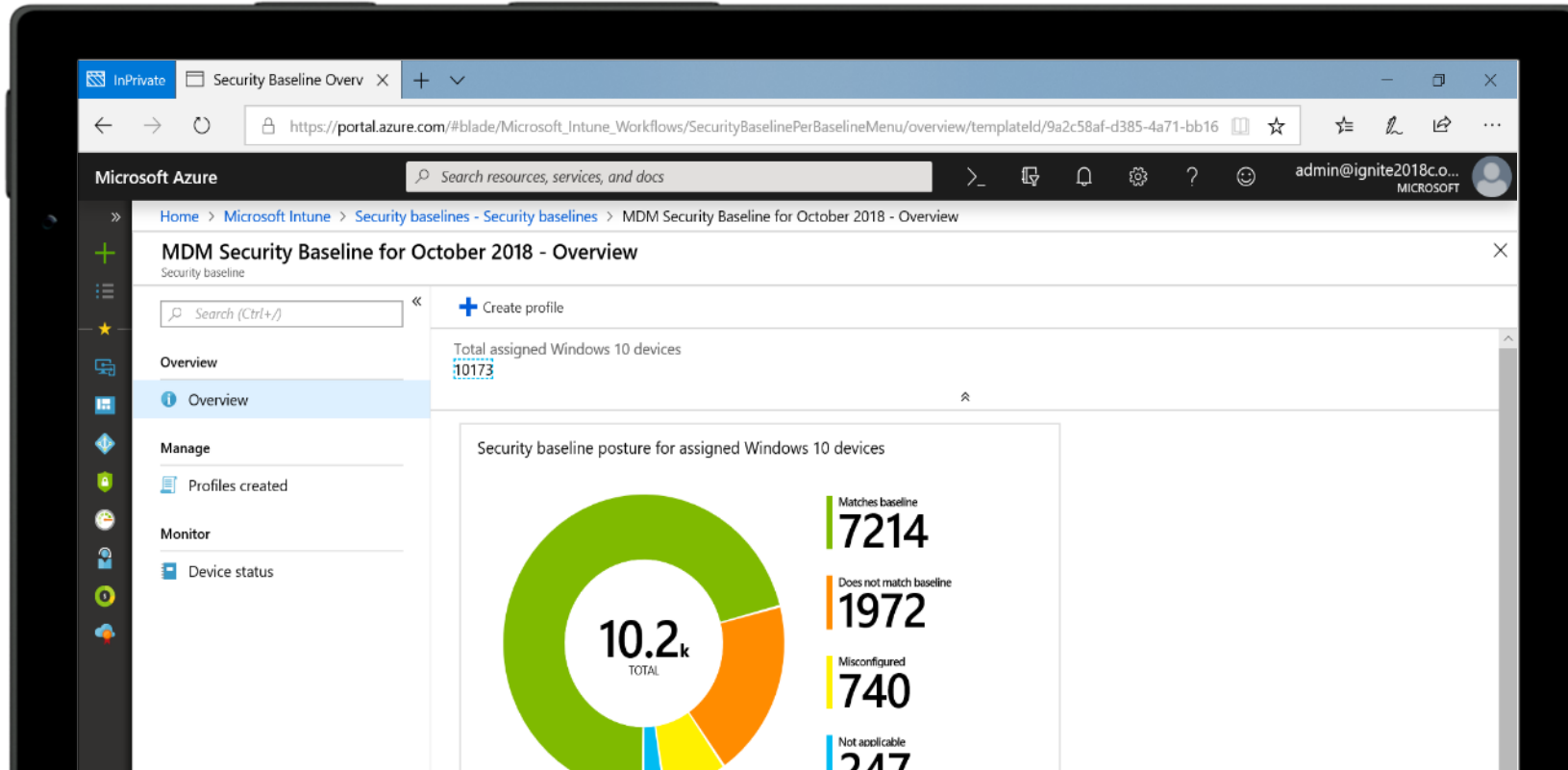


Microsoft Defender for Endpoint integration

Mobile threat defense (MTD) partners on iOS and Android



Improve security posture with cloud-powered analytics



Get insights from Microsoft cloud machine-learning



Simplify migration to Intune policy settings using security baselines



Monitor device compliance and automate remediation tasks

Stay secure with Microsoft Edge for iOS and Android

Designed for best secure browsing with Microsoft Intune policies



Security

Conditional Access
App Protection Policies



Productivity

Personal & Corporate
Identity Support
App Proxy, SSO



Manageability

Managed Favorites
& Home Shortcut
Blocked Sites





Accelerate Business Productivity

Fastest time to value



User-centered design for high user productivity

Comprehensive device settings ensure devices are productivity-ready with minimal user set-up.

Enrollment



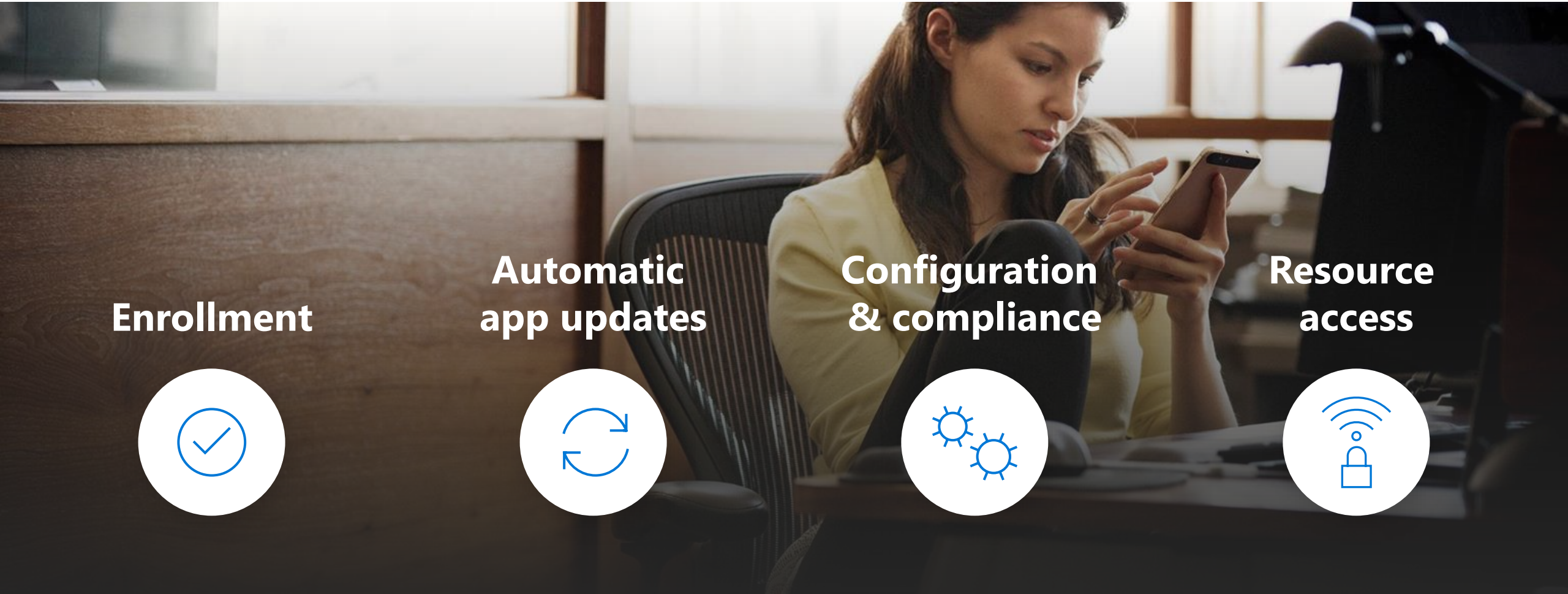
**Automatic
app updates**



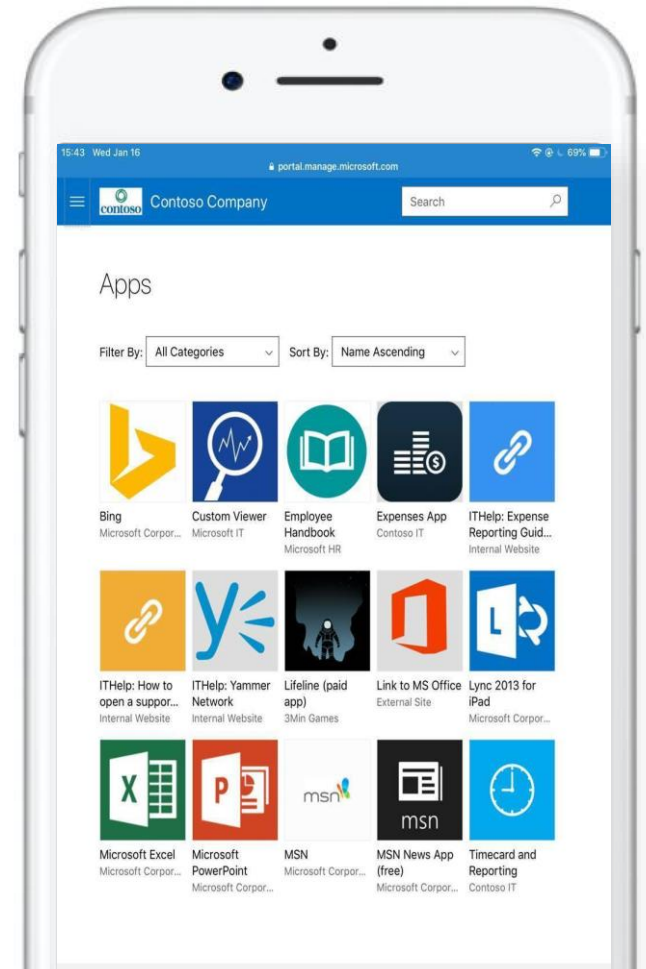
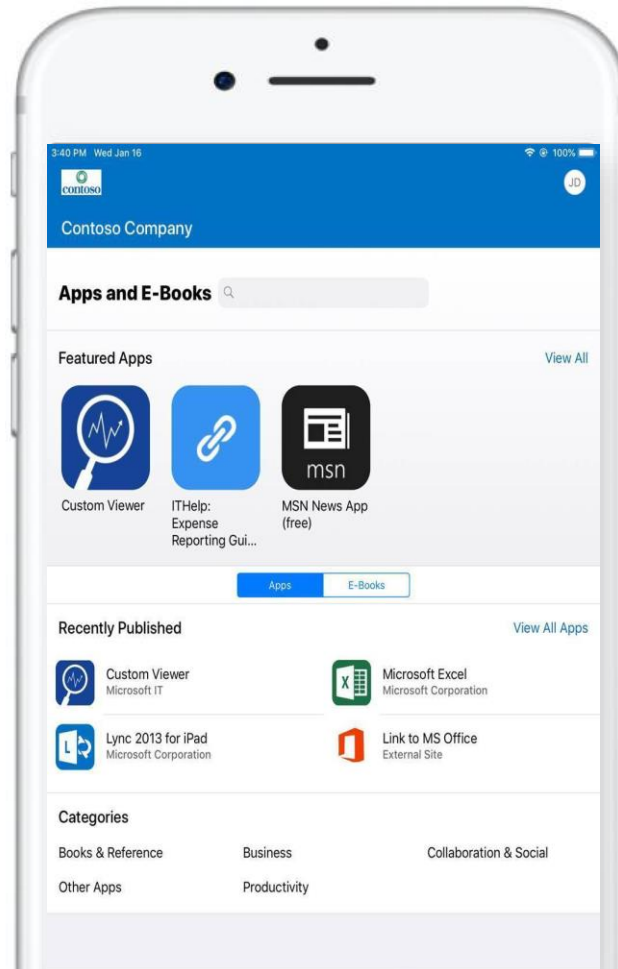
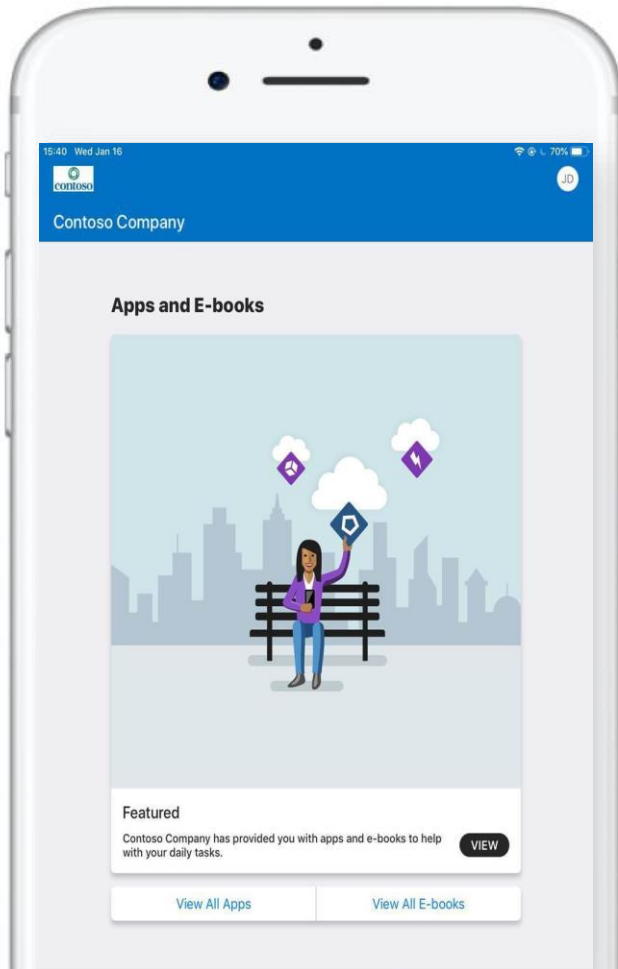
**Configuration
& compliance**



**Resource
access**



User-centered design in the new Company Portal app



Search apps & books
Search history

Enhanced filtering
with and without enrollment

Custom
branding

Native experience
without Safari WebView

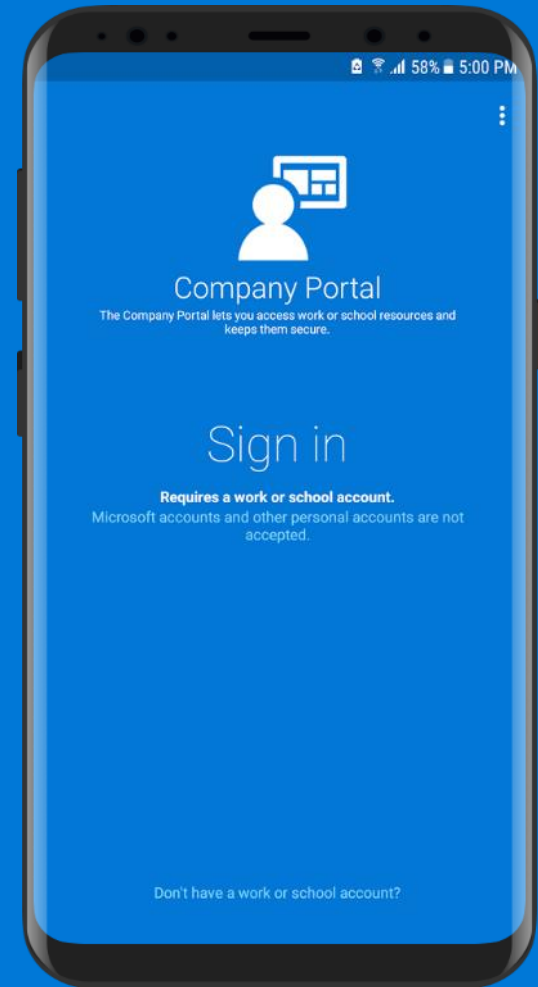
Self-service for more productivity, fewer support calls

User can **enroll or un-enroll devices** at their discretion using the Company Portal

Add **SaaS and public store apps** required by your organization

Use **self-service password** or PIN reset saving the user time and helpdesk costs

Join and manage groups without needing to go through IT

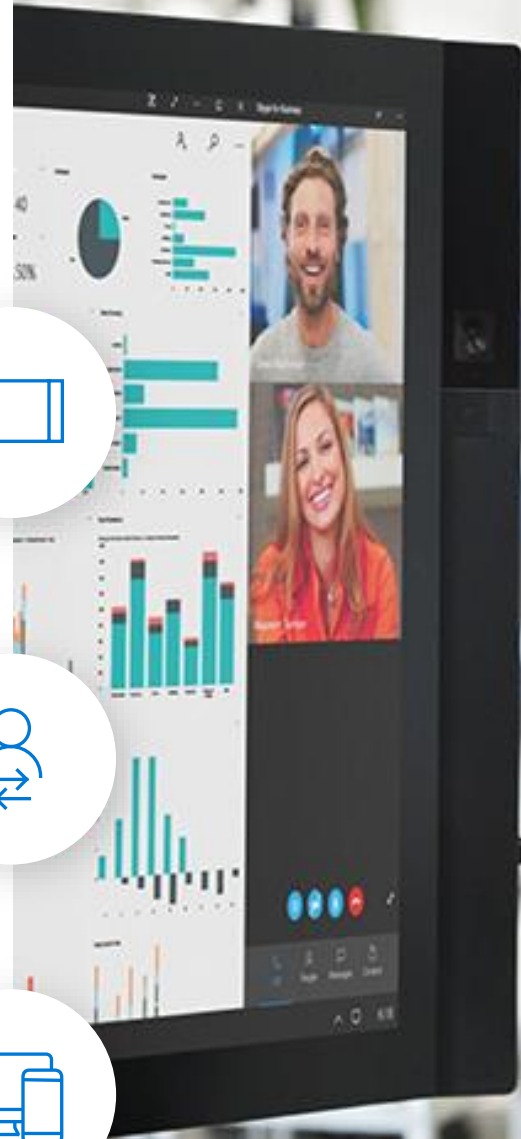
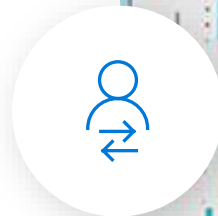
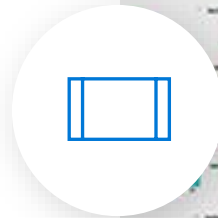


Enable more business scenarios

New **device-based subscription** to manage 'things' like digital signage, public kiosks, and phone room devices

Enable device management controls for devices **not affiliated with any user-identity** at a lower cost

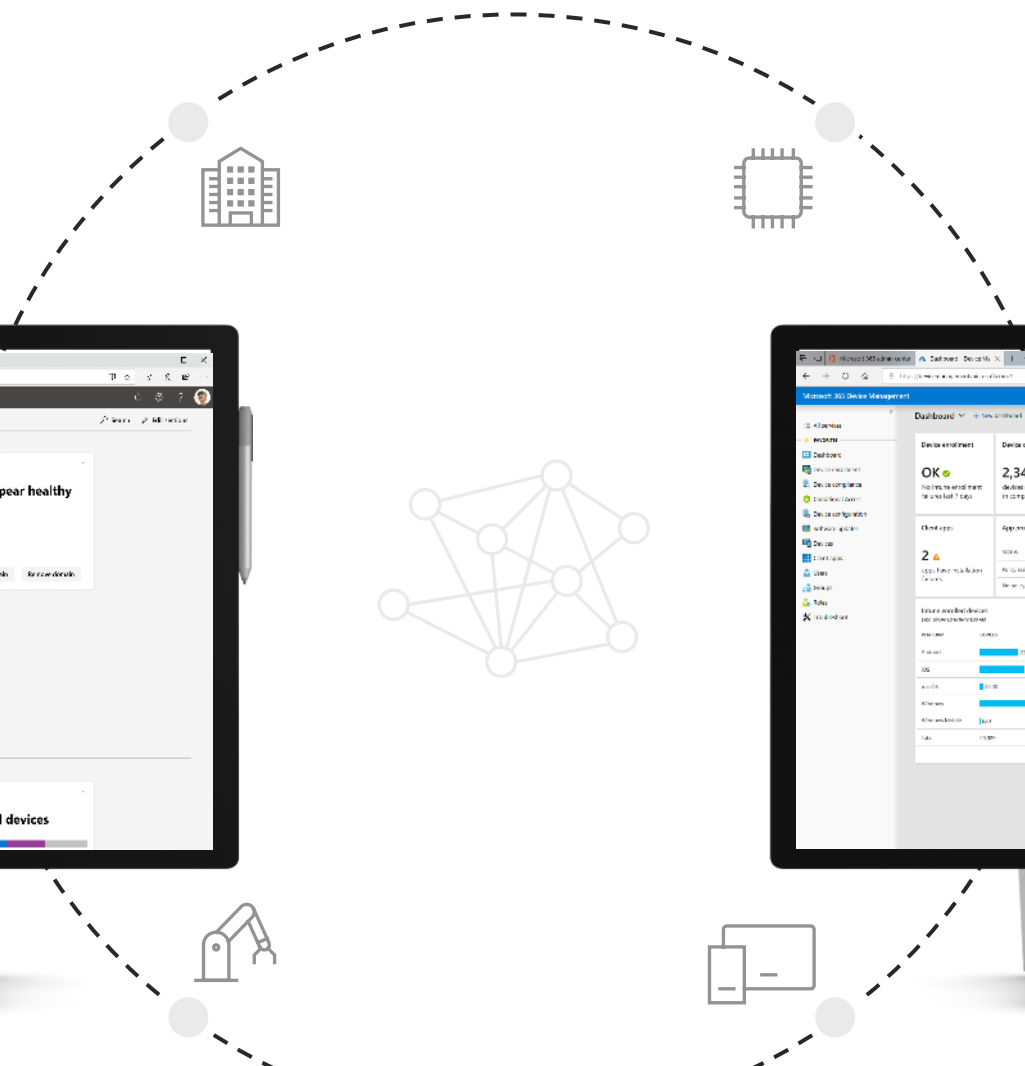
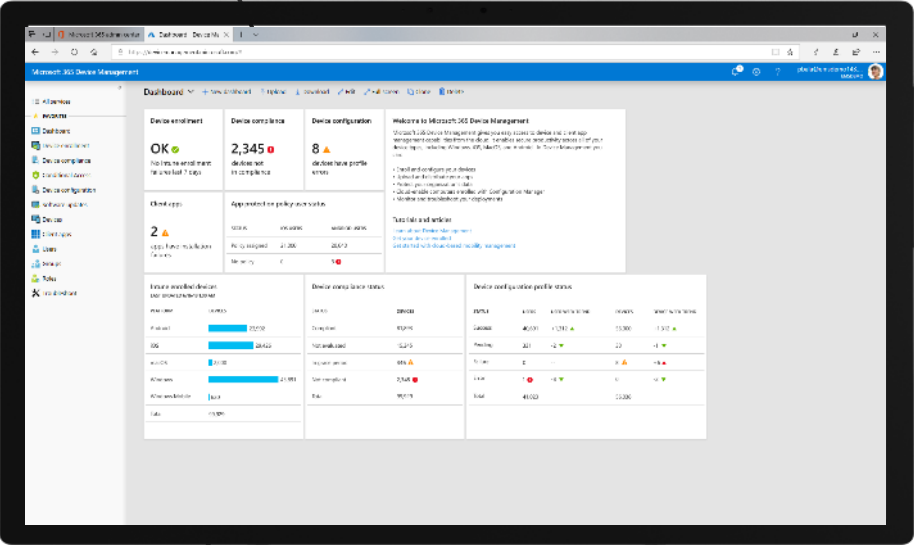
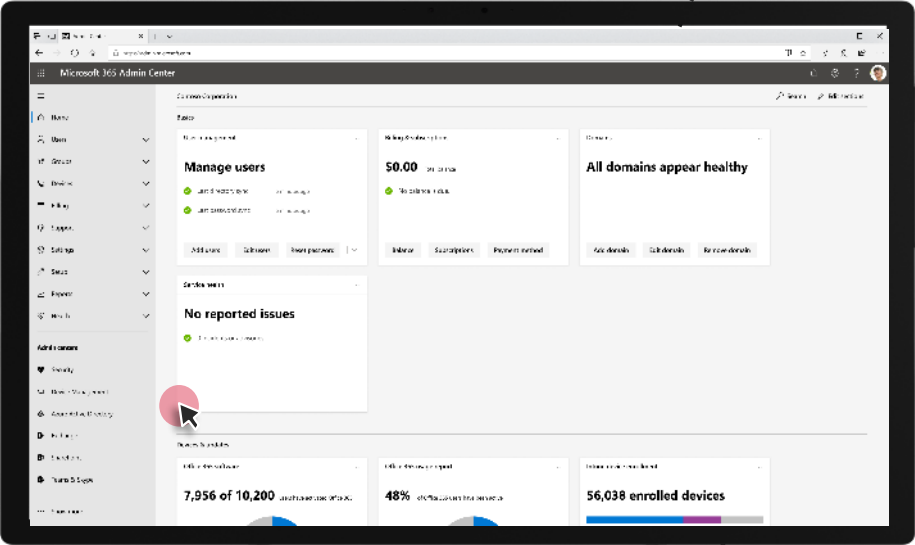
Works for **shared devices** used by multiple users without login



All endpoints managed from a Microsoft 365 console

Microsoft 365
Admin Center

Microsoft 365
Device Management



Microsoft Technology Partners

Intune integrated partners enhance the Microsoft 365 user experience and protect your company resources

MOBILE THREAT DEFENSE



SECURE RESOURCE ACCESS



MANAGEMENT PARTNERS



Microsoft device management is for all organizations



**Knowledge
Workers**

Microsoft 365
Enterprise



**Firstline
Workers**

Microsoft 365
F1



**SMB
Employee**

Microsoft 365
Business



**Teachers/
Students**

Microsoft 365 Education
(Intune for Education)

Microsoft recognized as a **Leader***

175M+ managed devices worldwide

115M+ seats installed base

* Source: Gartner, Magic Quadrant for Unified Endpoint Management Tools, Chris Silva, Manjunath Bhat, et al, 6 August 2019

Disclaimer: This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from <https://aka.ms/IntuneMQ>

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Figure 1. Magic Quadrant for Unified Endpoint Management



Source: Gartner (August 2019)

© Gartner, Inc

Microsoft Intune compliance offerings

Help comply with requirements governing collection and use of individual's data

Global



ISO 27001



ISO 27018



ISO 27017



ISO 22301



SOC 1 Type 2



SOC 2 Type 2



SOC 3



CSA STAR Self-Assessment



CSA STAR Certification



CSA STAR Attestation

Regional



Argentina PDPA



EU Model Clauses



UK G-Cloud



China DJCP



China GB 18030



China TRUCS



Singapore MTCS



Australia IRAP/CCSL



New Zealand GCIO



Japan My Number Act



ENISA IAF



Japan CS Mark Gold



Spain ENS



Spain DPA



India MeitY



Canada Privacy Laws



Privacy Shield



Germany IT Grundschutz workbook

Industry



PCI DSS Level 1



CDSA



MPAA



FACT UK



Shared Assessments



FISC Japan



HIPAA/HITECH Act



HITRUST



GxP 21 CFR Part 11



MARS-E



IG Toolkit UK



FERPA



GLBA



FFIEC

Us Gov



Moderate JAB P-ATO



High JAB P-ATO



DoD DISA SRG Level 2



DoD DISA SRG Level 4



DoD DISA SRG Level 5



SP 800-171



FIPS 140-2



Section 508 VPAT



ITAR



CJIS



IRS 1075

Key Takeaways



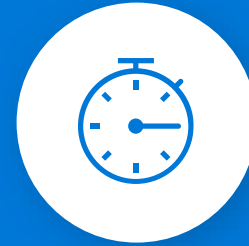
Most complete

Microsoft Endpoint Manager delivers most complete management of modern workplace



Most secure

Extensive cloud powered insights and policy-driven actions for the most secure protection of your data



Fastest time to value

Remove barriers to productivity on any personal and company-owned devices without compromising security



Thank you.