Microsoft 365

AGiLiS®

Endpoint Management Workshop

Unified endpoint management to secure the modern workplace

Cem Ersoy
Solution Sales Specialist
Agilis Teknoloji Çözümleri

Technology needs are evolving in the modern workplace

Fragmented → Integrated

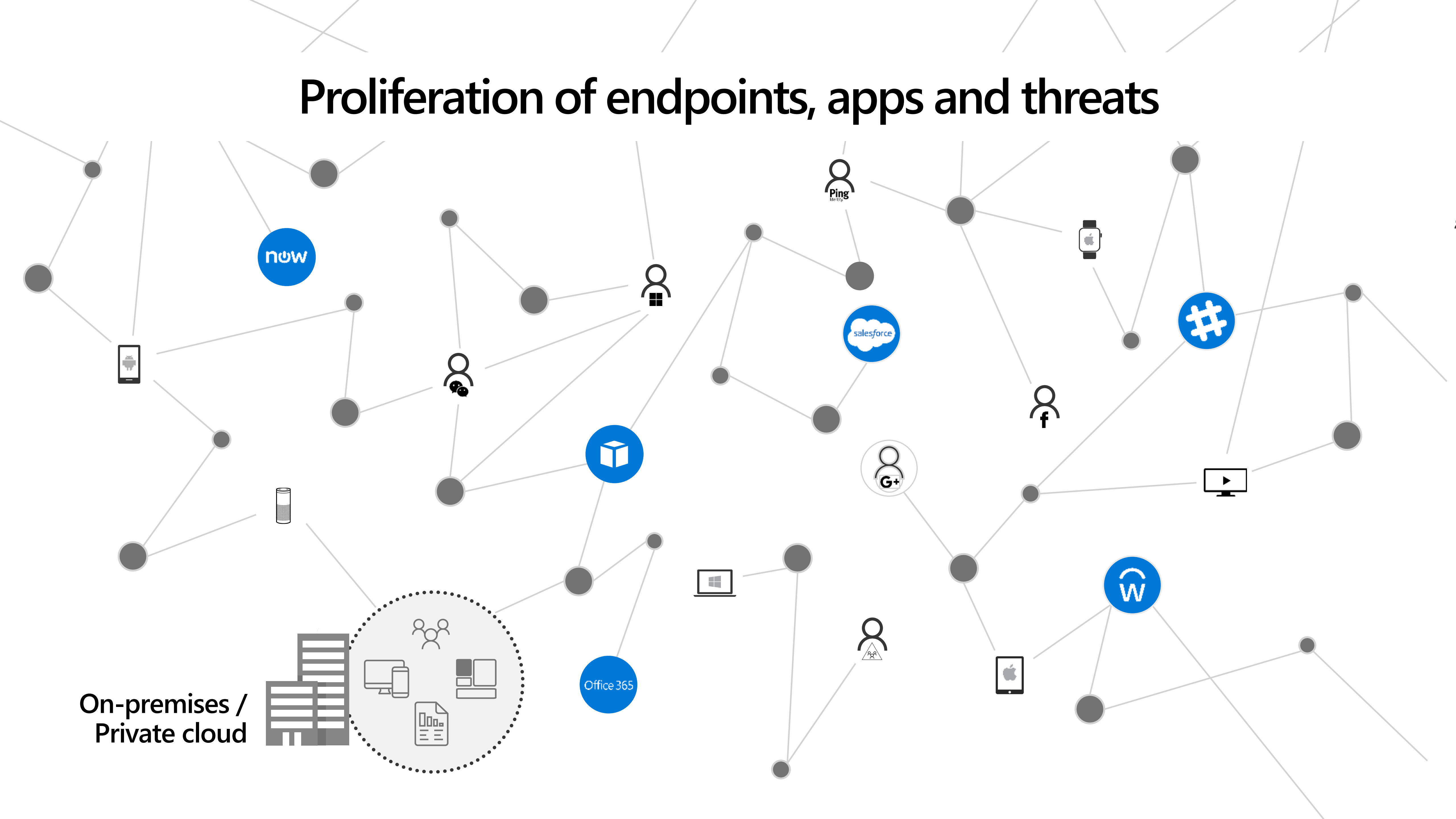
Closed Perimeter → Cloud

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?

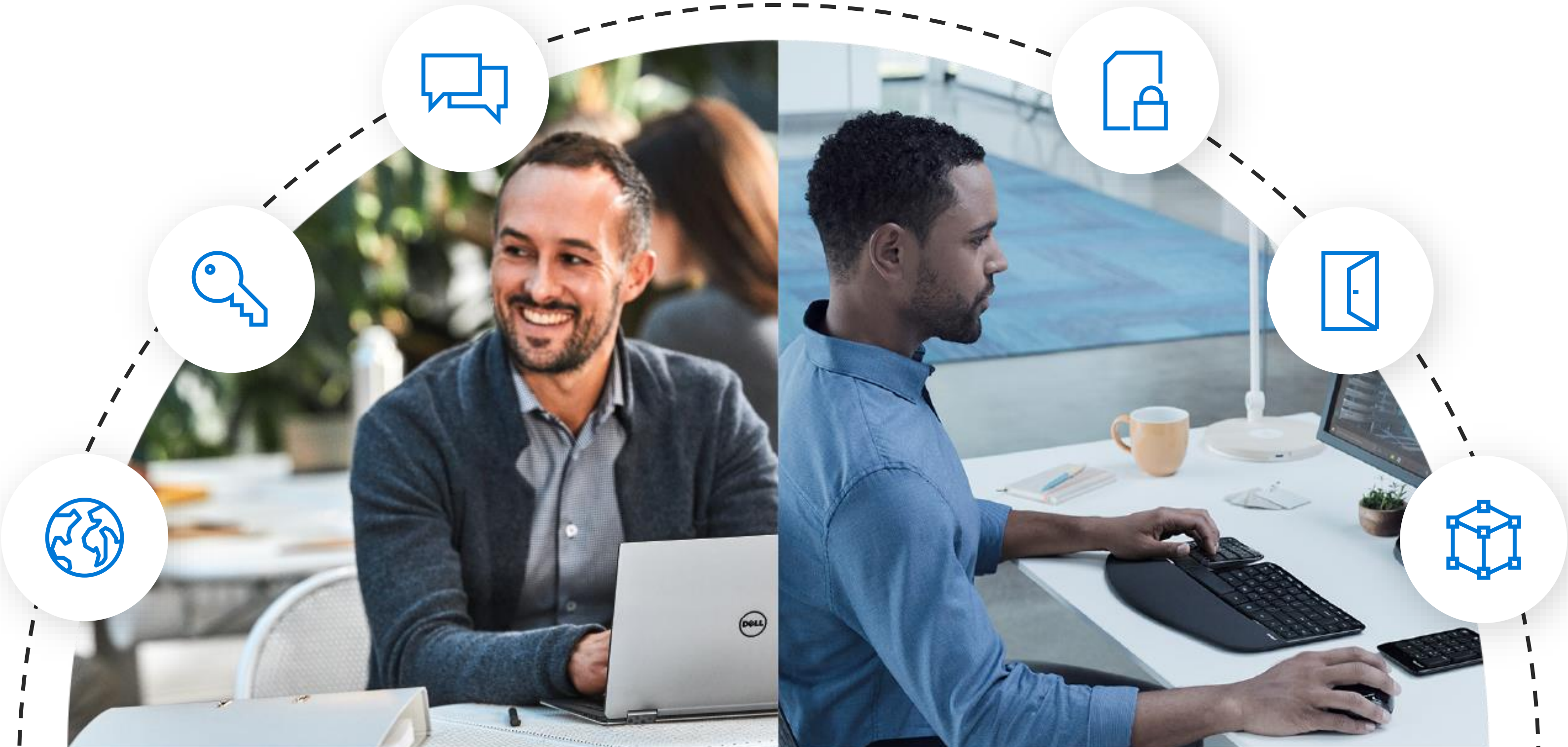
Employee goals

IT goals

Collaborate

Easy access

Work anywhere



Protect data

Manage access

Stay innovative

Transformative device management and security

Microsoft Flexible Device Management

Enable your users

Protect your data

PC desktop management

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

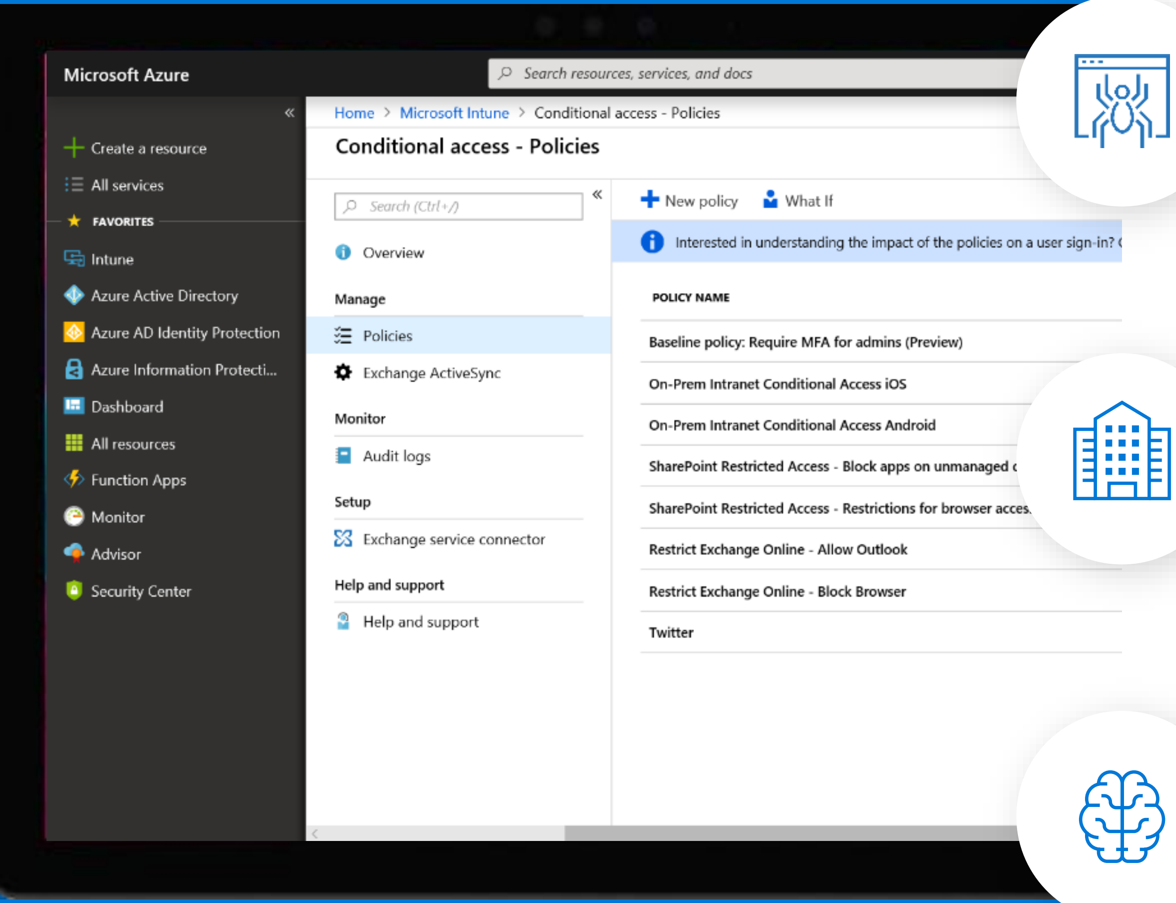
Transform IT delivery and device management

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



Interested in understanding the impact of the policies on a user sign-in?

POLICY NAME
Baseline policy: Require MFA for admins (Preview)
On-Prem Intranet Conditional Access iOS
On-Prem Intranet Conditional Access Android
SharePoint Restricted Access - Block apps on unmanaged
SharePoint Restricted Access - Restrictions for browser acces
Restrict Exchange Online - Allow Outlook
Restrict Exchange Online - Block Browser
Twitter

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

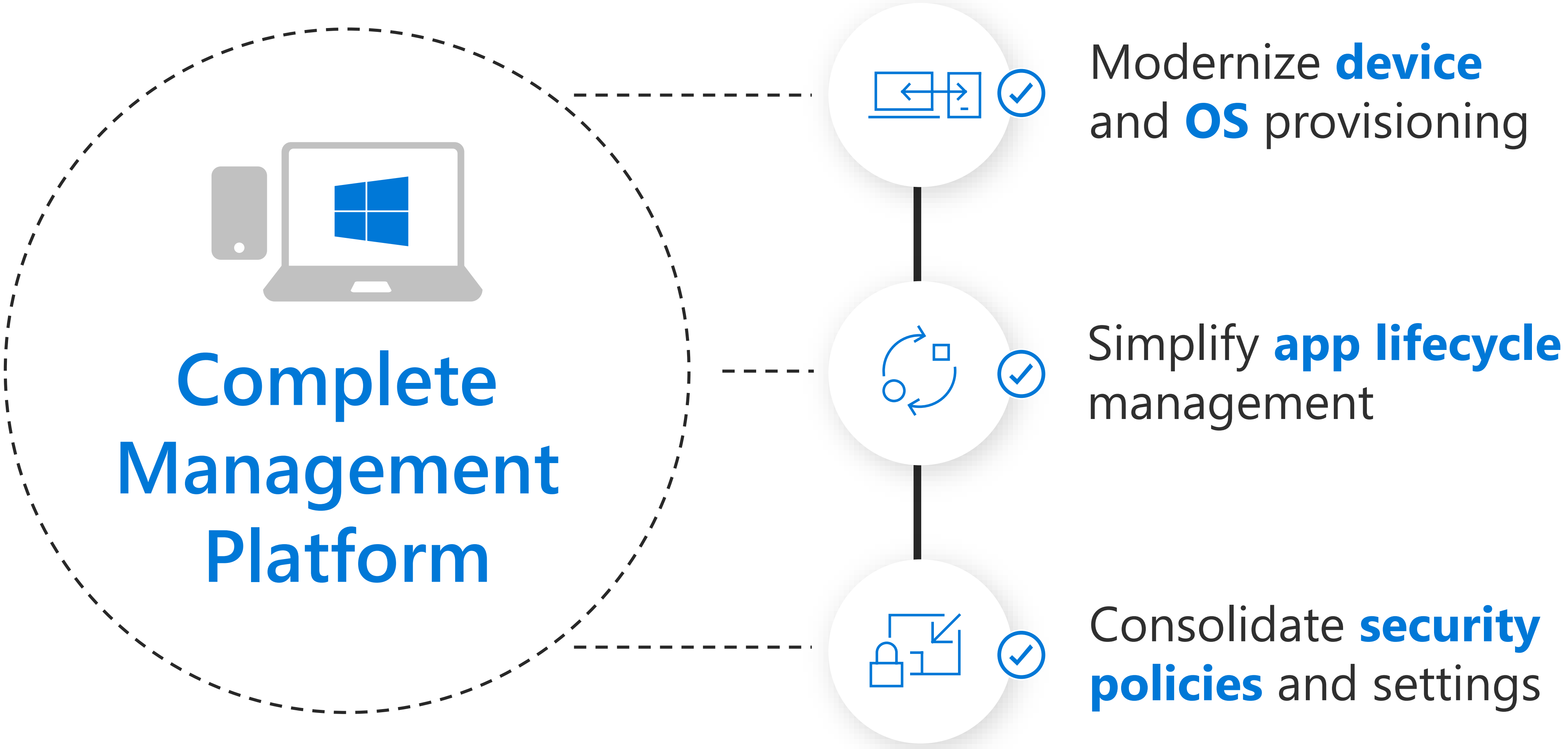
Simplify **access to resources** employees need with single sign-on, for faster service roll-out

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



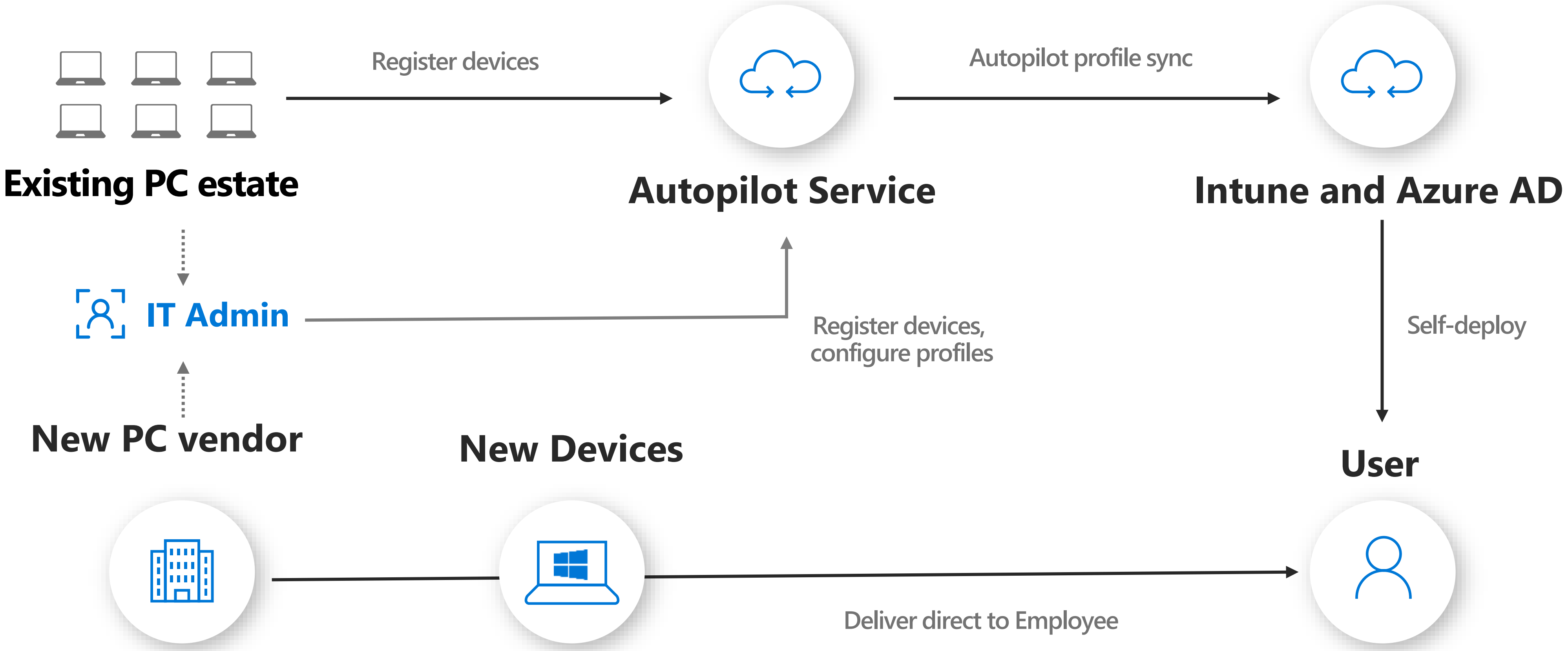
Complete Management Platform

Modernize **device** and **OS** provisioning

Simplify **app lifecycle** management

Consolidate **security policies** and settings

Modern desktop provisioning with Windows Autopilot

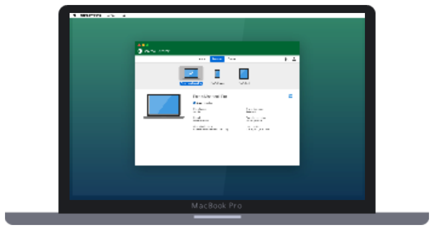


- ✓ Provision new devices direct to employees, ready for use
- ✓ Upgrade existing devices, reimaged with Autopilot
- ✓ Lower IT effort and cost; user gets productive faster

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

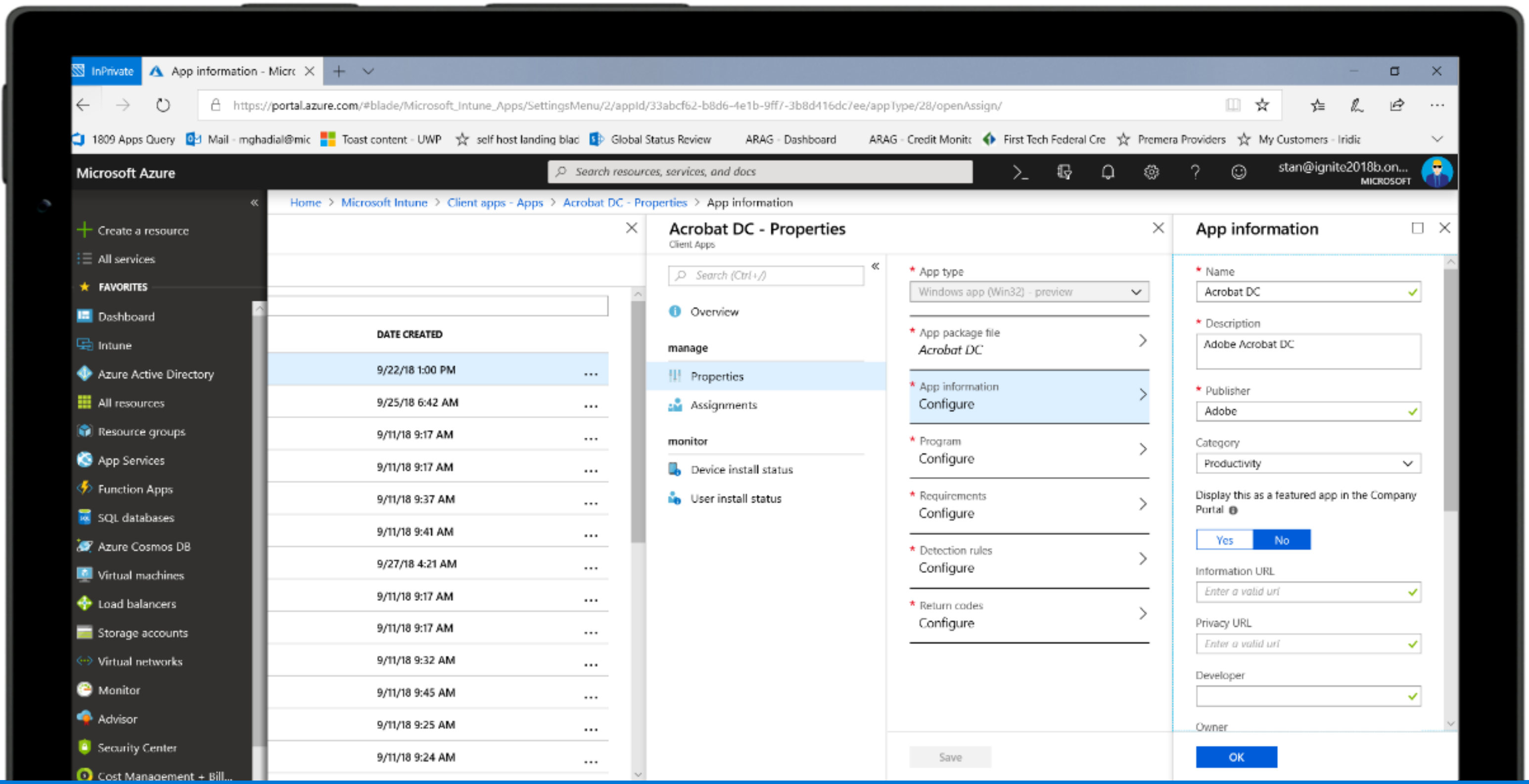
(with Jamf)

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



DATE CREATED
9/22/18 1:00 PM
9/25/18 6:42 AM
9/11/18 9:17 AM
9/11/18 9:17 AM
9/11/18 9:37 AM
9/11/18 9:41 AM
9/27/18 4:21 AM
9/11/18 9:17 AM
9/11/18 9:17 AM
9/11/18 9:32 AM
9/11/18 9:45 AM
9/11/18 9:25 AM
9/11/18 9:24 AM

Acrobat DC - Properties
Client Apps

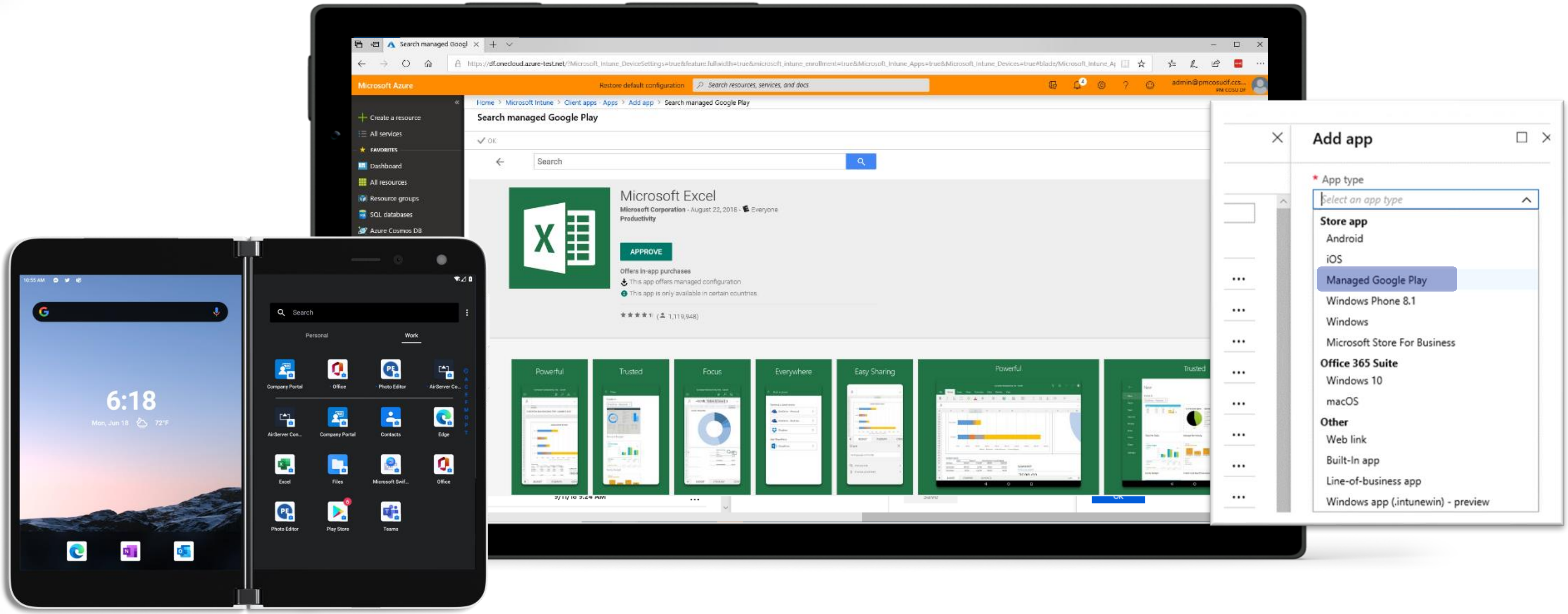
* App type: Windows app (Win32) - preview
* App package file: Acrobat DC
* App information: Configure
* Program: Configure
* Requirements: Configure
* Detection rules: Configure
* Return codes: Configure

App information

* Name: Acrobat DC
* Description: Adobe Acrobat DC
* Publisher: Adobe
Category: Productivity
Display this as a featured app in the Company Portal: Yes [✓ No]
Information URL: Enter a valid url
Privacy URL: Enter a valid url
Developer:
Owner

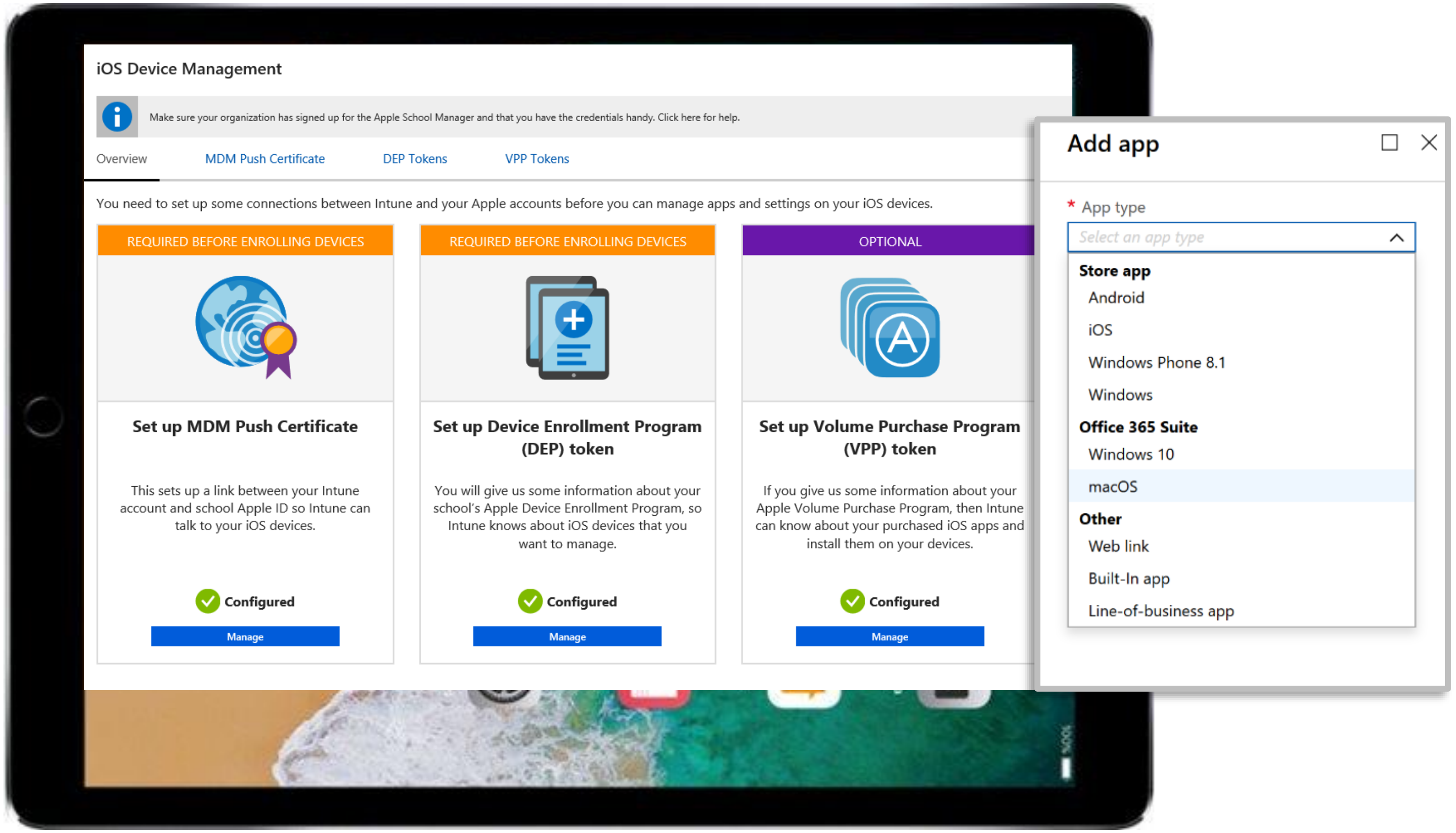
- Deploy Win32 apps, line-of-business (LOB) apps, and Microsoft store apps from the cloud
- Application compatibility assurance using desktop analytics
- Intune leverages Windows 10 cloud management capabilities

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



iOS Device Management

Make sure your organization has signed up for the Apple School Manager and that you have the credentials handy. Click here for help.

Overview | MDM Push Certificate | DEP Tokens | VPP Tokens

You need to set up some connections between Intune and your Apple accounts before you can manage apps and settings on your iOS devices.

REQUIRED BEFORE ENROLLING DEVICES

Set up MDM Push Certificate

This sets up a link between your Intune account and school Apple ID so Intune can talk to your iOS devices.

✓ Configured

Manage

REQUIRED BEFORE ENROLLING DEVICES

Set up Device Enrollment Program (DEP) token

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.

✓ Configured

Manage

OPTIONAL

Set up Volume Purchase Program (VPP) token

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.

✓ Configured

Manage

Add app

* App type

Select an app type

Store app
- Android
- iOS
- Windows Phone 8.1
- Windows

Office 365 Suite
- Windows 10
- macOS

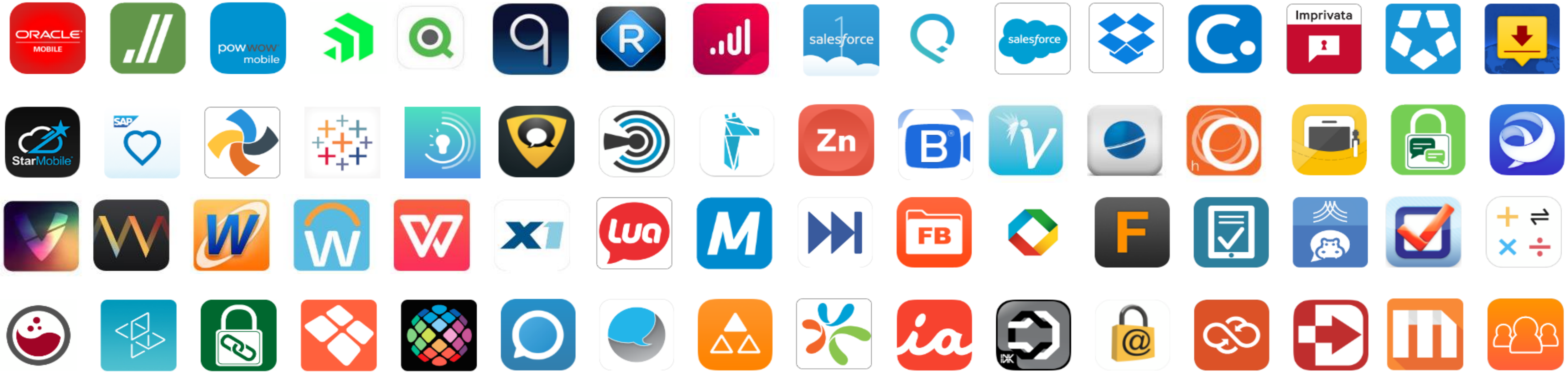
Other
- Web link
- Built-In app
- Line-of-business app

✓ 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



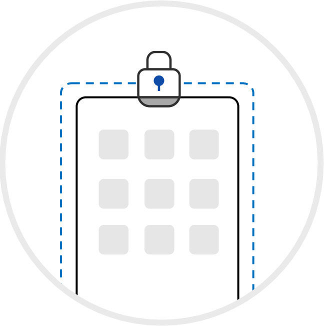
Most Trusted Workplace

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

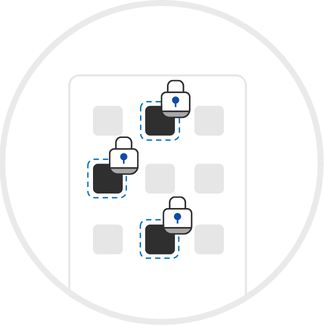
Provision settings, certs, profiles

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



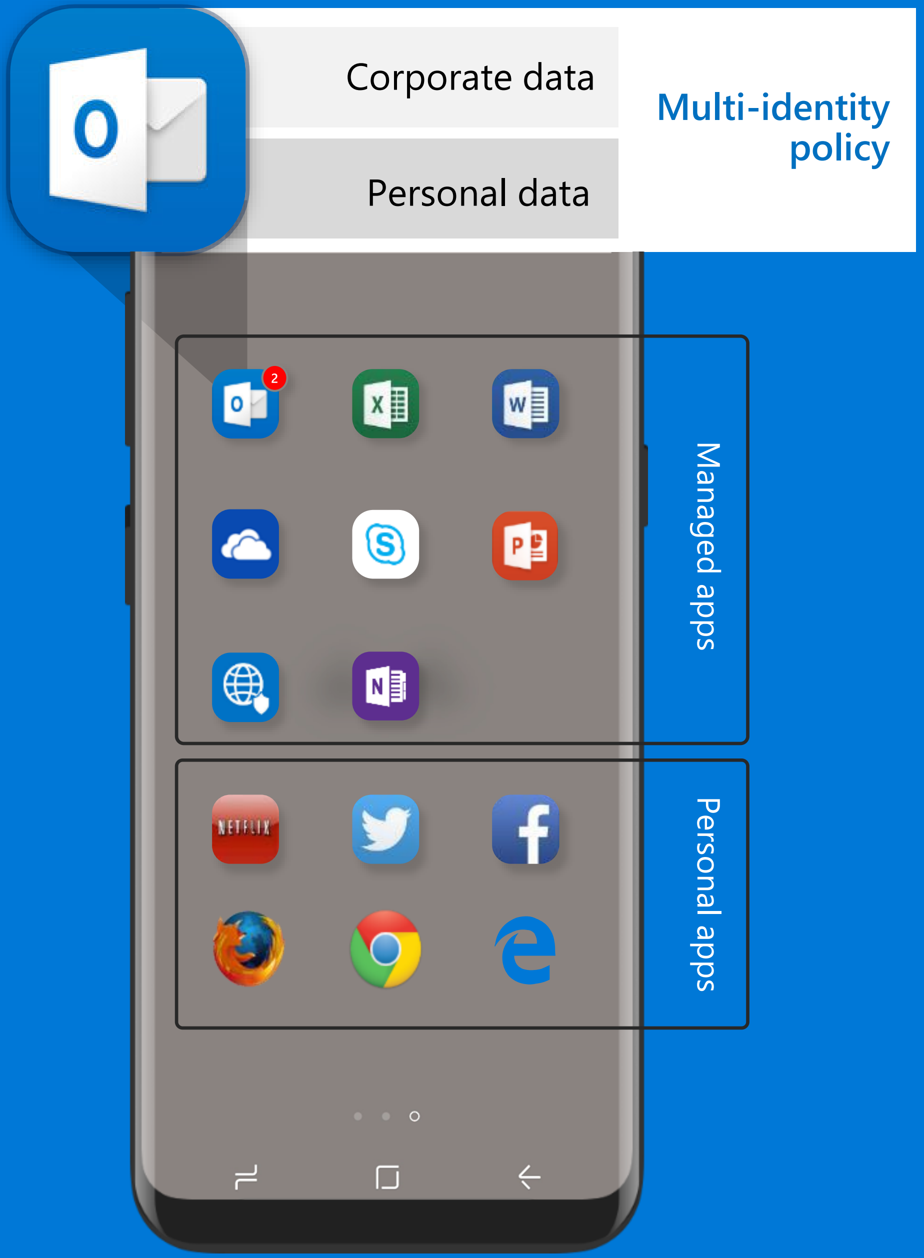
Publish mobile apps to users

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.

box
babs
SAP
Skype for Business

Check back frequently…

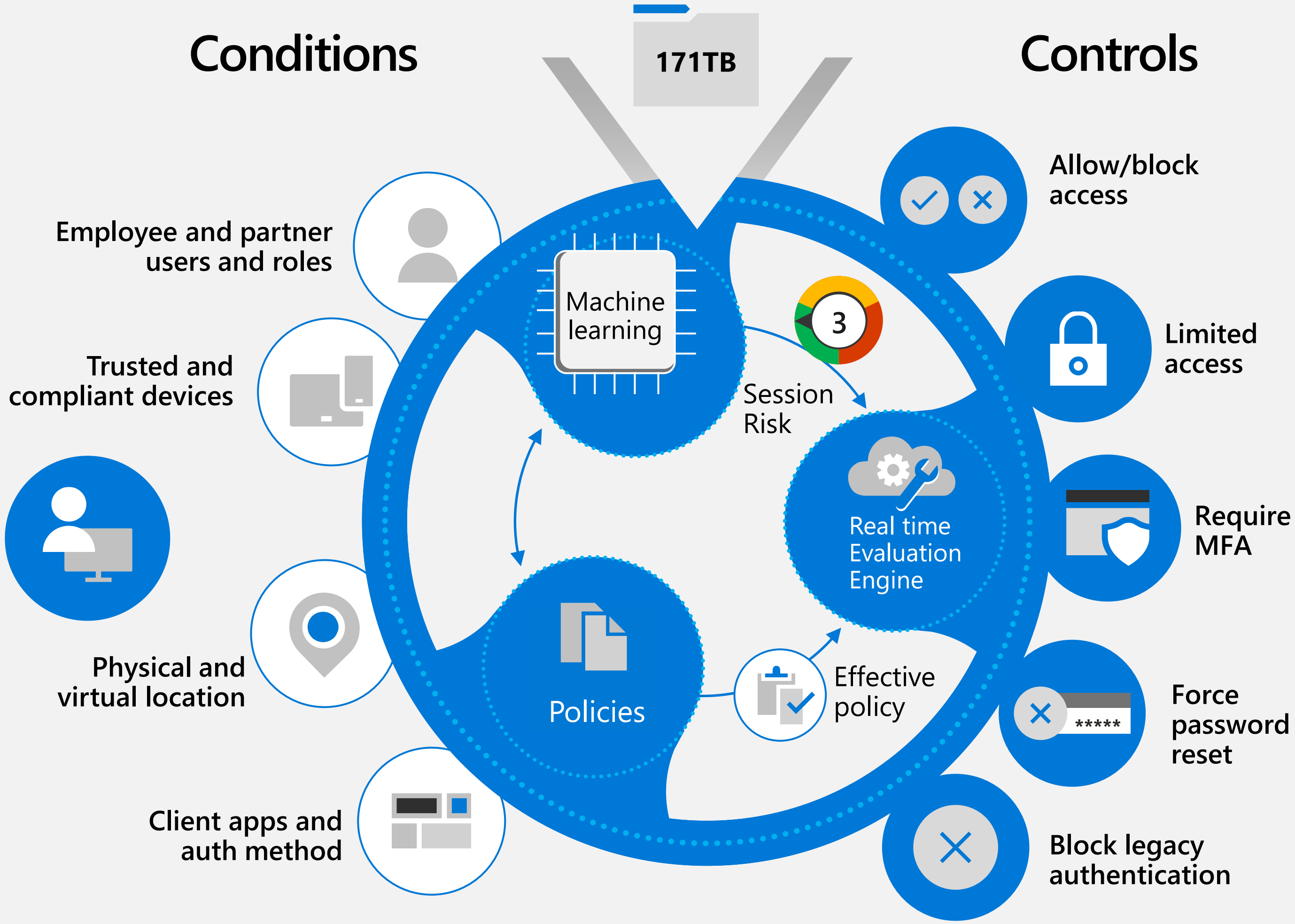
we are constantly adding new apps to this list

Conditional access to data with real-time risk analysis

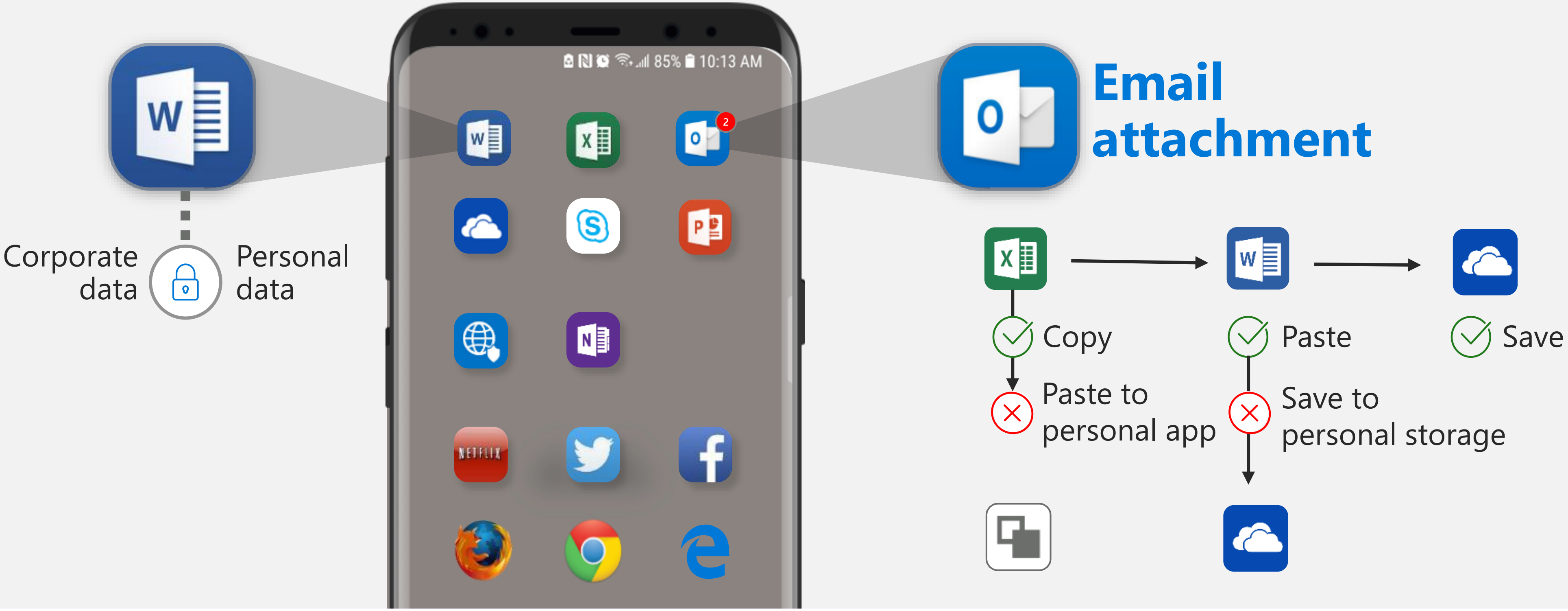
Define **contextual policies** at the user, location, device, and app levels

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

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


Conditions
171TB
Controls
Employee and partner users and roles
Trusted and compliant devices
Physical and virtual location
Client apps and auth method
Machine learning
3
Session Risk
Real time Evaluation Engine
Policies
Effective policy
Allow/block access
Limited access
Require MFA
Force password reset
*****
Block legacy authentication

Control what happens after data has been accessed

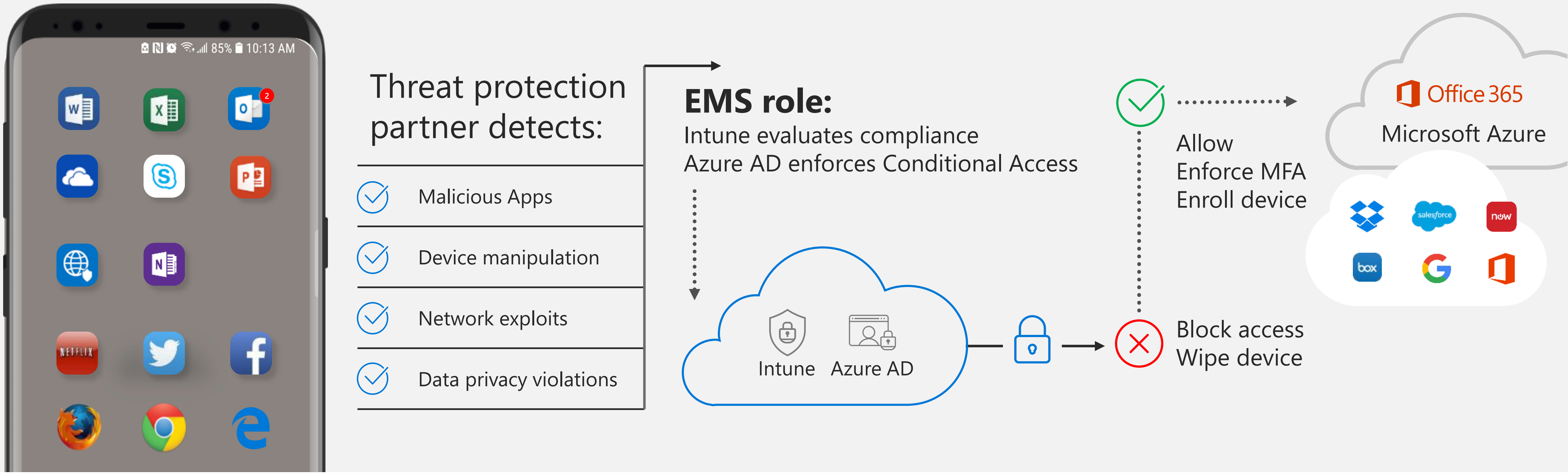


Microsoft Information Protection (MIP) empowers you to **control how data is accessed** from employee devices

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

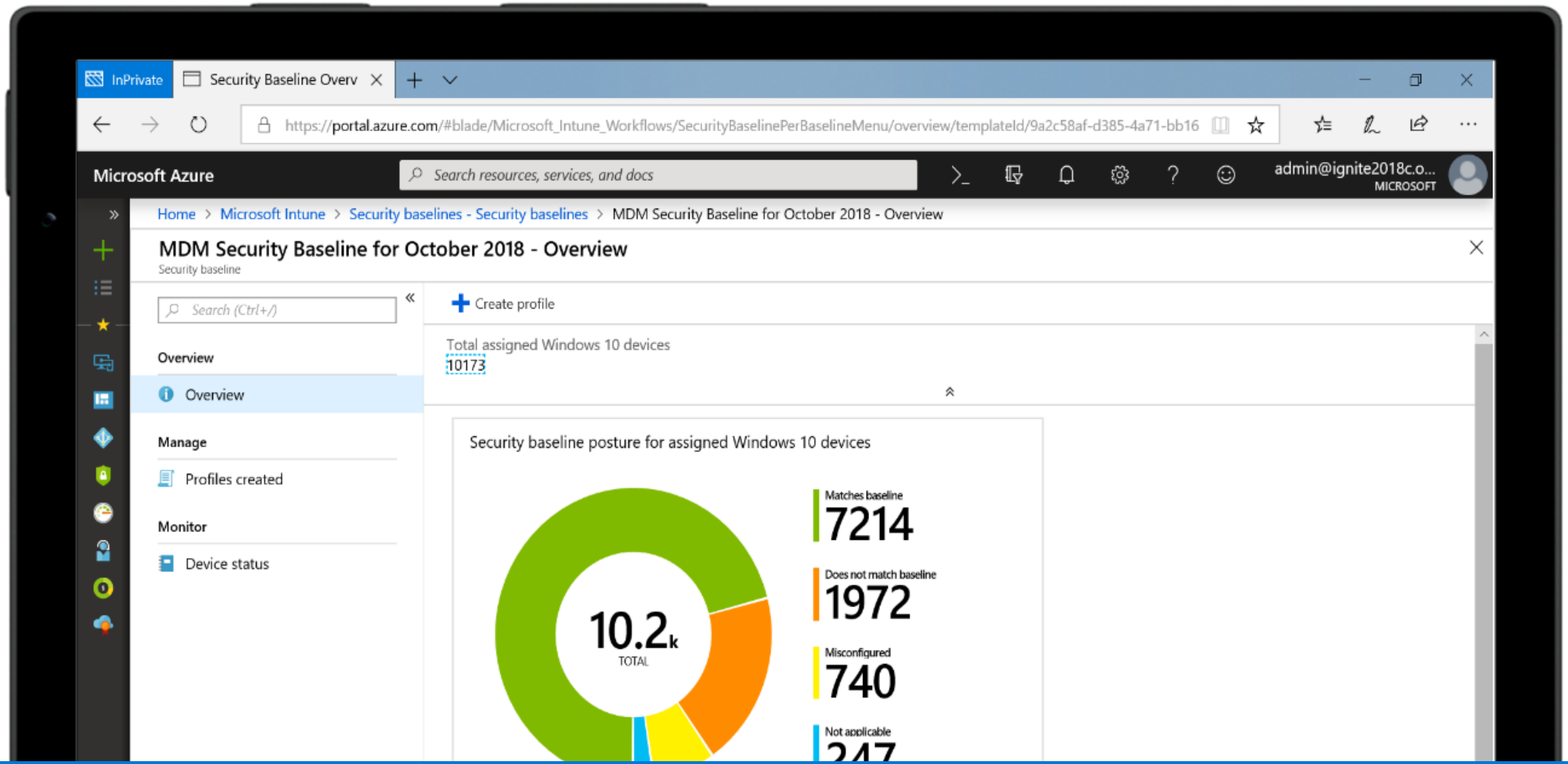
✕ Block access
Wipe device

Microsoft Defender for Endpoint integration

Mobile threat defense (MTD) partners on iOS and Android

Microsoft
Lookout
Symantec.
ZIMPERIUM.
pradeo
Google Play Protect
Check Point SOFTWARE TECHNOLOGIES LTD

Improve security posture with cloud-powered analytics


InPrivate
Security Baseline Overv
https://portal.azure.com/#blade/Microsoft_Intune_Workflows/SecurityBaselinePerBaselineMenu/overview/templateId/9a2c58af-d385-4a71-bb16
Microsoft Azure
Search resources, services, and docs
admin@ignite2018c.o...
MICROSOFT
Home > Microsoft Intune > Security baselines - Security baselines > MDM Security Baseline for October 2018 - Overview
MDM Security Baseline for October 2018 - Overview
Security baseline
Search (Ctrl+/)
Overview
Overview
Manage
Profiles created
Monitor
Device status
Create profile
Total assigned Windows 10 devices
10173
Security baseline posture for assigned Windows 10 devices
10.2k
TOTAL
Matches baseline
7214
Does not match baseline
1972
Misconfigured
740
Not applicable
247

- 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

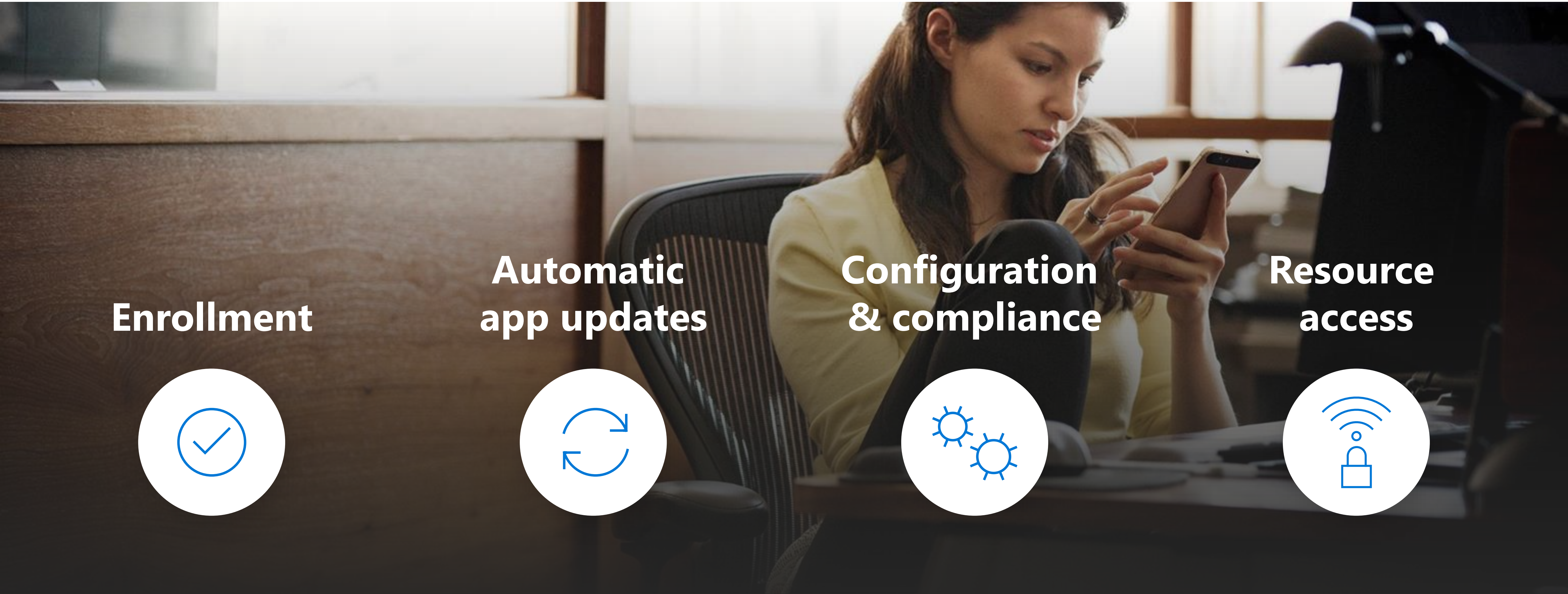
Favorites
Favorites Bar
Skype | Free calls to friends and family
https://www.skype.com/en/
Lonely Planet
https://www.lonelyplanet.com/
Mail - mona@outlook.com
https://outlook.live.com/owa/
Condé Nast Traveler - Travel Reviews
https://www.cntraveler.com/
Nordstrom Online & In Store: Shoes, J...
https://m.shop.nordstrom.com/
Thrillist - Find the Best and Most Unc...
http://www.thrillist.com/
MSN.com - Hotmail, Outlook, Skype...
http://www.msn.com/
The Future Is Now by Mic | Tech powe...
Back
9:41 AM
Better veggies. Better living.
RECIPES
fast 'n healt
Classic Ma
Pizza with
Fresh Mo

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.



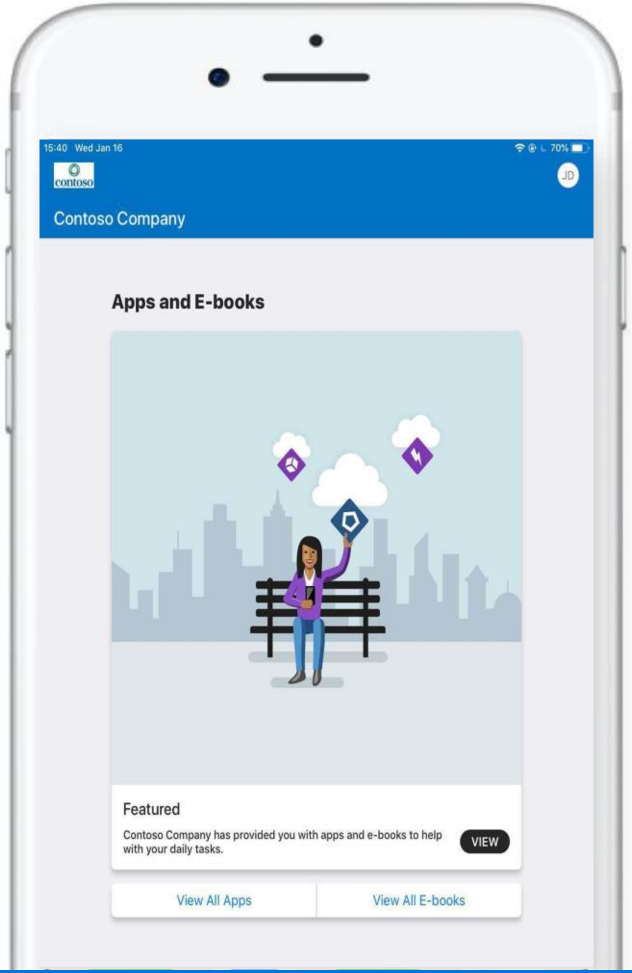
Enrollment

Automatic app updates

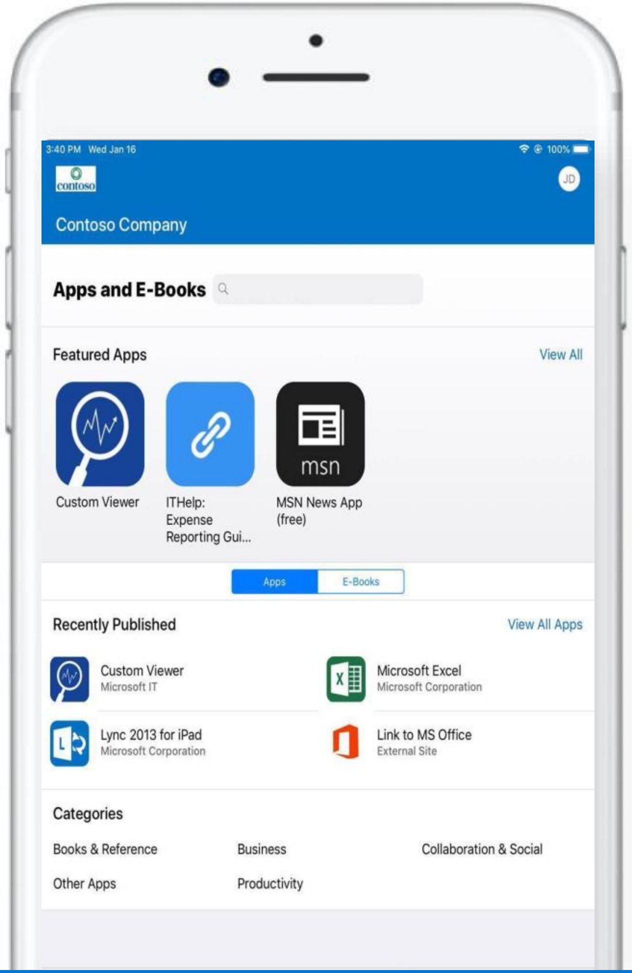
Configuration & compliance

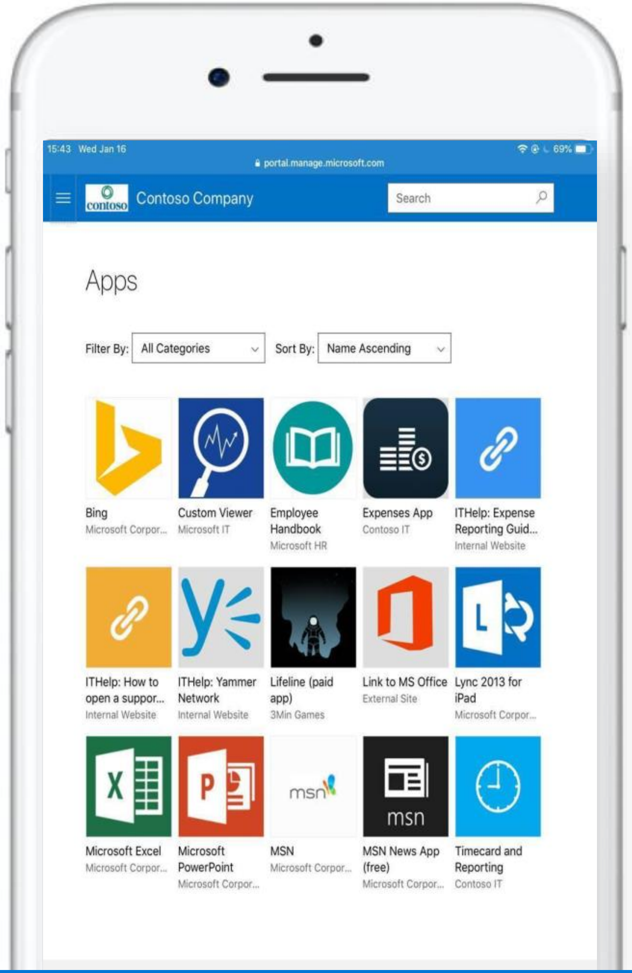
Resource access

User-centered design in the new Company Portal app



Contoso Company has provided you with apps and e-books to help with your daily tasks.





Search apps & books
Search history

Enhanced filtering
with and without enrollment

Custom
branding

Native experience
without Safari WebView

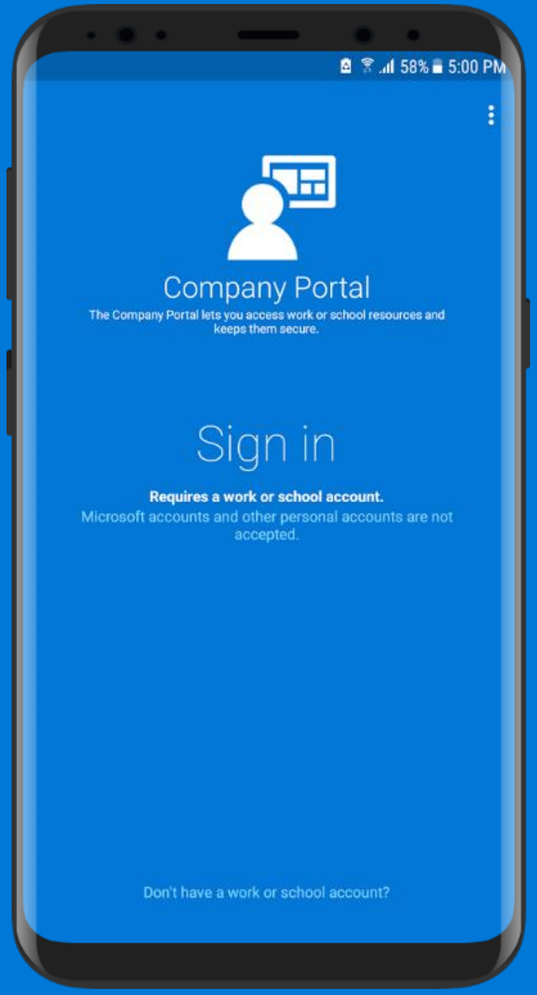
Self-service for more productivity, fewer support calls

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



Company Portal

The Company Portal lets you access work or school resources and keeps them secure.

Sign in

Requires a work or school account.

Microsoft accounts and other personal accounts are not accepted.

Don't have a work or school account?

Enable more business scenarios

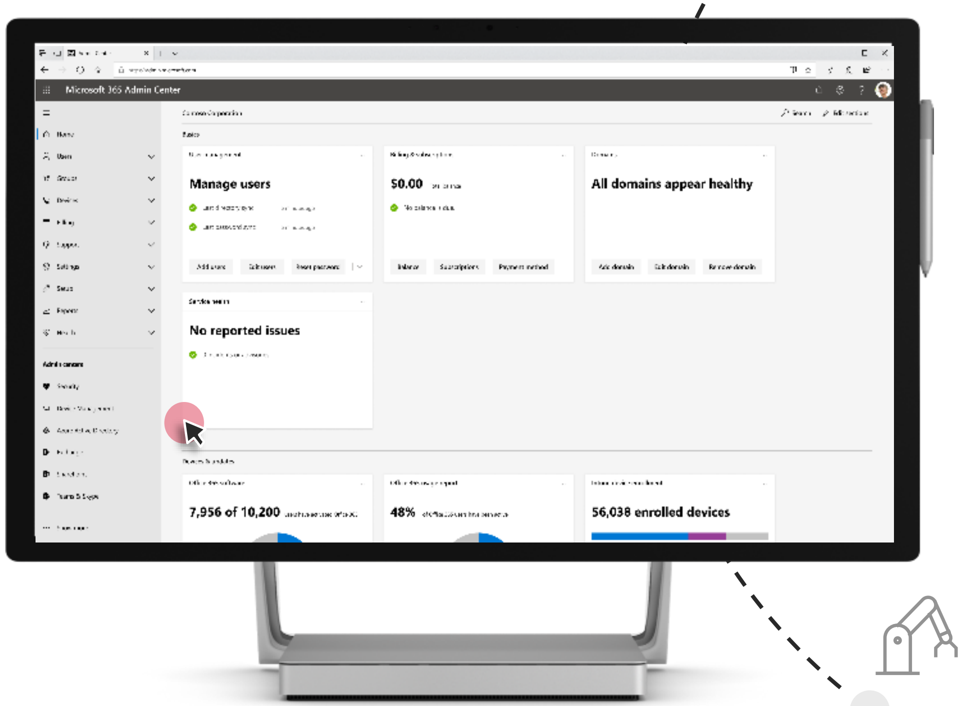
New **device-based subscription** to manage ‘things’ like digital signage, public kiosks, and phone room devices

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

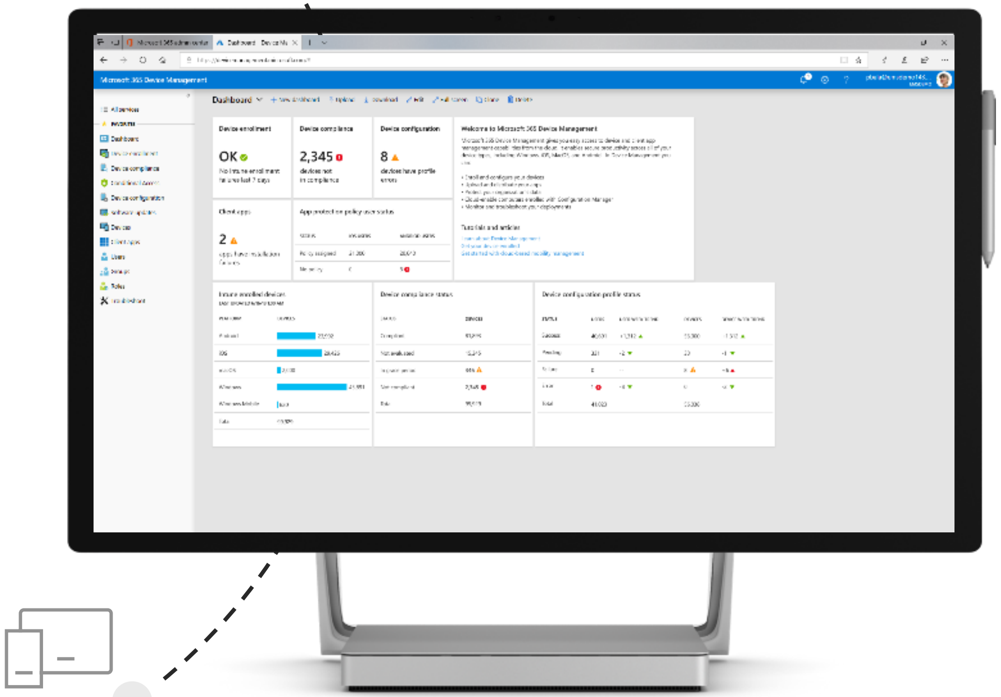
Works for **shared devices** used by multiple users without login

All endpoints managed from a Microsoft 365 console

Microsoft 365 Admin Center



Microsoft 365 Device Management


Microsoft 365 Device Management
Dashboard
Device enrollment
OK
Device compliance
2,345
devices not in compliance
Device configuration
8
devices have profile errors
Welcome to Microsoft 365 Device Management
Client apps
2
App protection policy user status
Tutorials and articles
Intune enrolled devices
Device compliance status
Device configuration profile status

Microsoft Technology Partners

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

MOBILE THREAT DEFENSE

Lookout

Symantec.

pradeo

ZIMPERIUM.

Check Point
SOFTWARE TECHNOLOGIES LTD

SECURE RESOURCE ACCESS

CITRIX®

IDNOMIC

digicert®

CISCO.

GlobalSign.
GMO INTERNET GROUP

Entrust Datacard™

zscaler™

MANAGEMENT PARTNERS

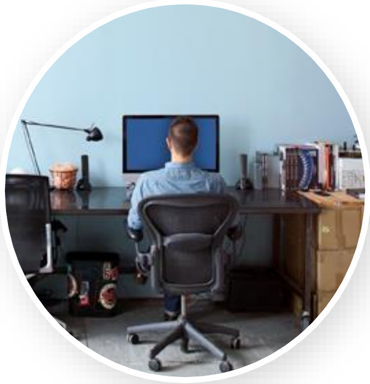
jamf

APACHE CORDOVA™

DATALERT

wandera

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

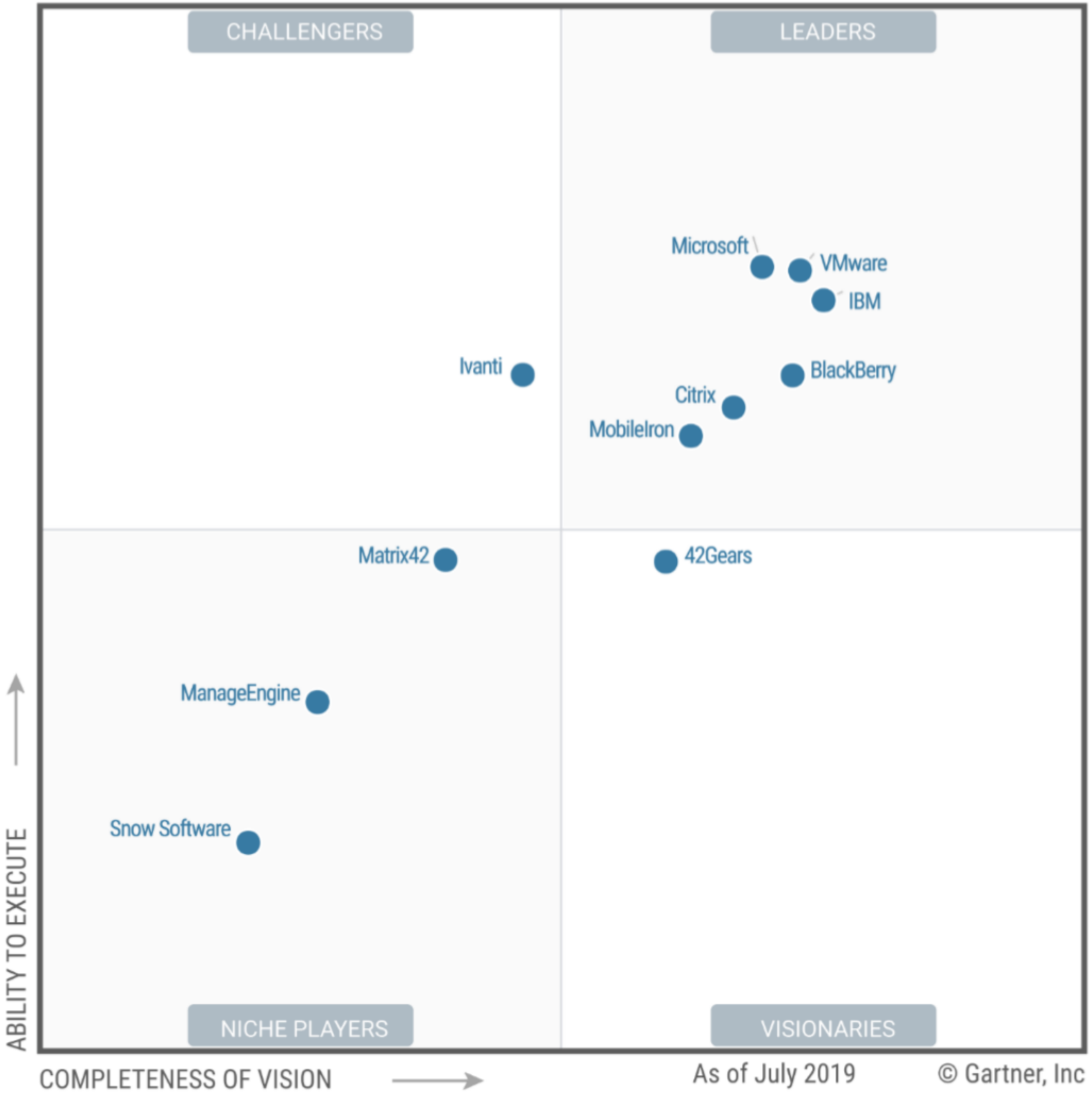
115M+ seats installed base

* 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)

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

Microsoft 365

Thank you.