
MICROSERVE
Modern Management
Introduction

# Transformative device management and security

Microsoft Flexible Device Management

**Enable your users**

PC desktop management

Mobile device management

**Protect your data**

Mobile application management

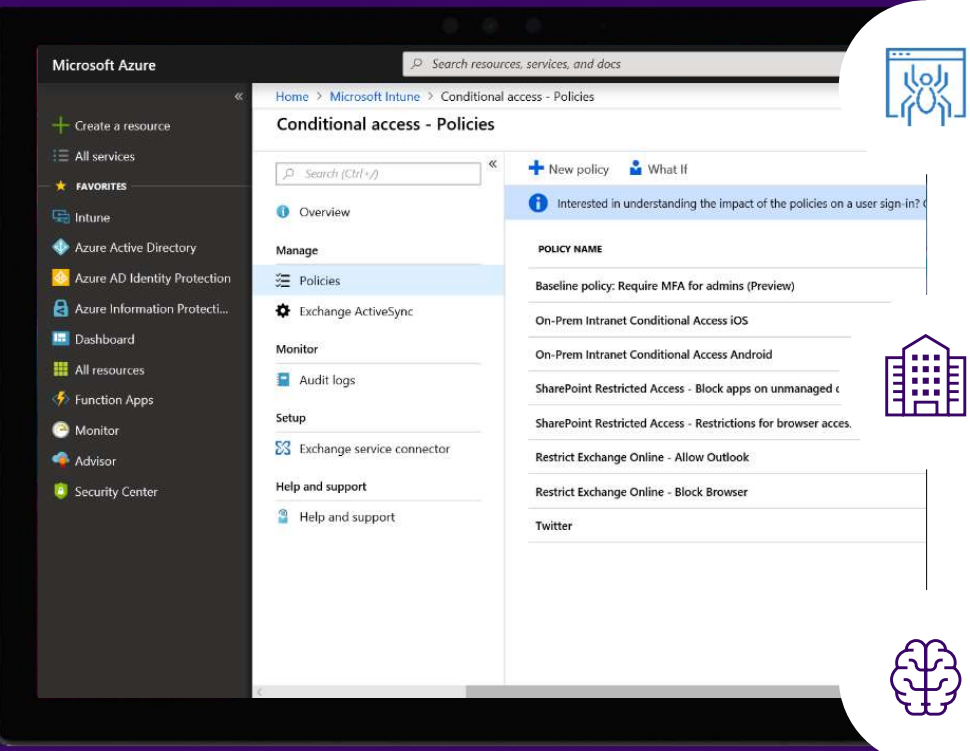
SERVE

# 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

MICROSERVE

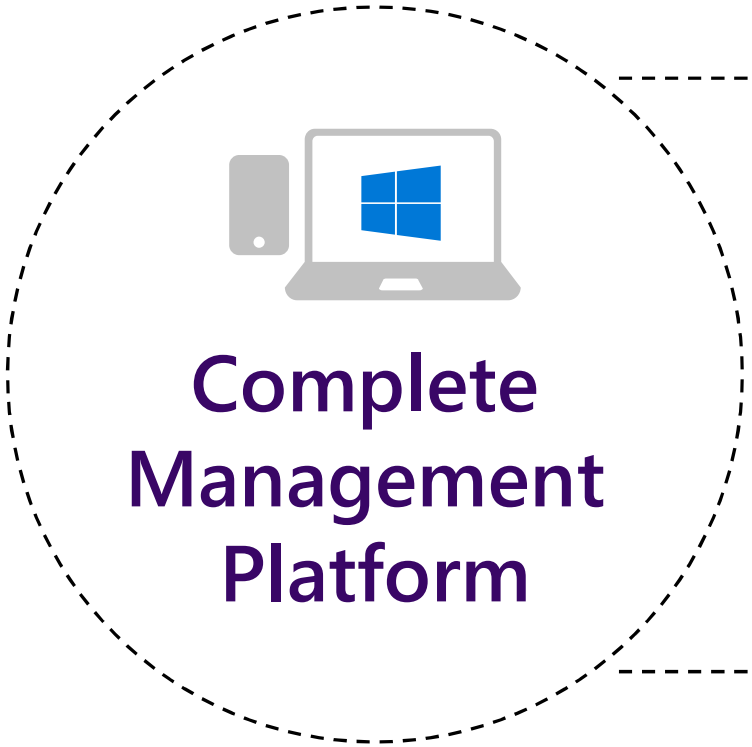
# Maximize user productivity

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

# Microsoft simplifies mobile and PC management




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

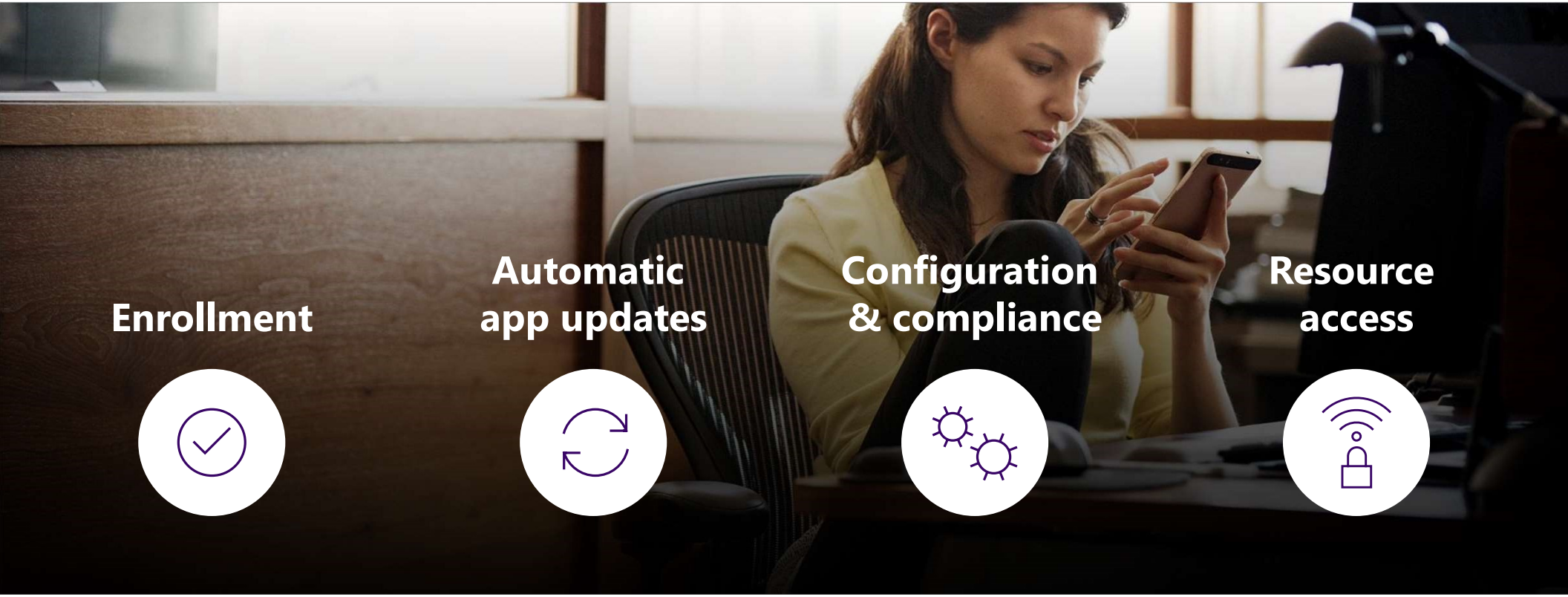
Simplify **app lifecycle** management

Consolidate **security policies** and settings

MICROSERVE

# Microsoft simplifies mobile and PC management

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



# Microsoft recognized as a Leader*

**175M+** managed devices worldwide

**115M+** seats installed base

Figure 1. Magic Quadrant for Unified Endpoint Management


Source: Gartner (August 2019)

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

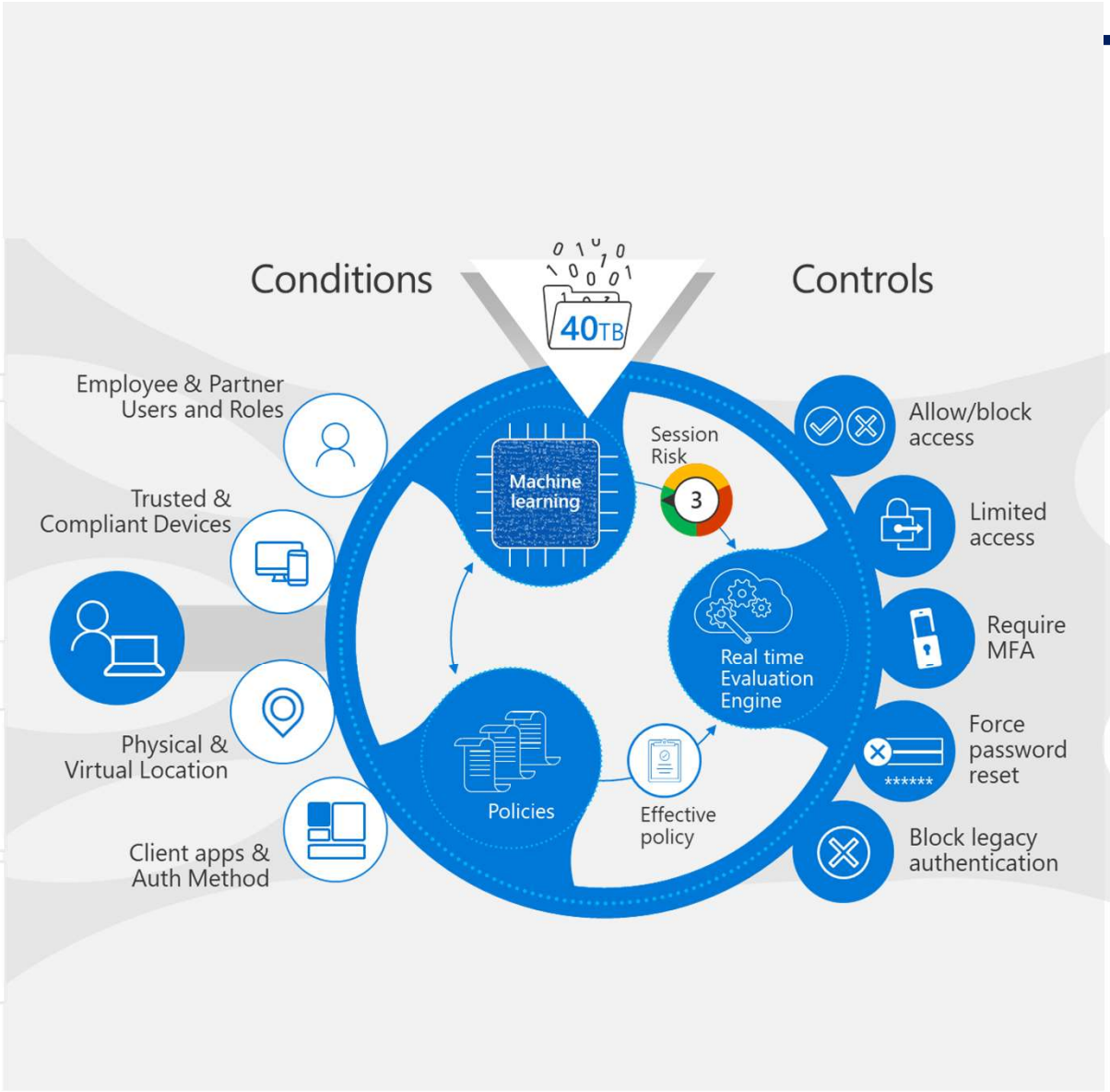

HOW MODERN MANAGEMENT
WORKS
MICROSERVE

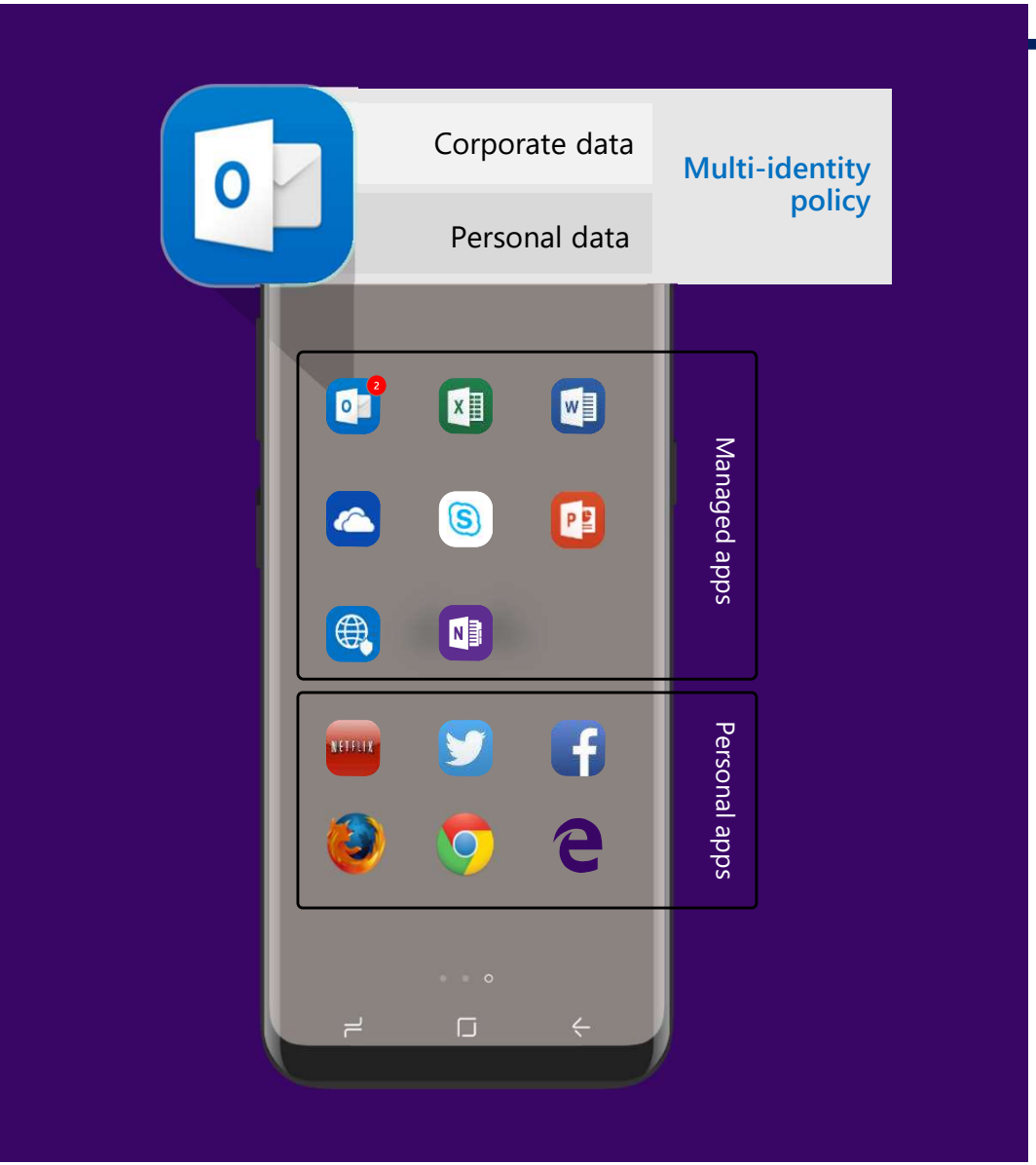
# Conditional access to data with real-time risk analysis

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**






# 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

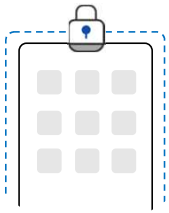
**Intune App Protection policies** are useful to protect Microsoft 365 apps where devices are unmanaged or managed by 3rd party

MICROSERVE

# Protect your data on virtually any device with Intune

## Mobile **Device** Management (MDM)

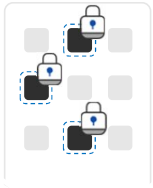
**Conditional Access:**
Restrict access to managed and compliant devices



- 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

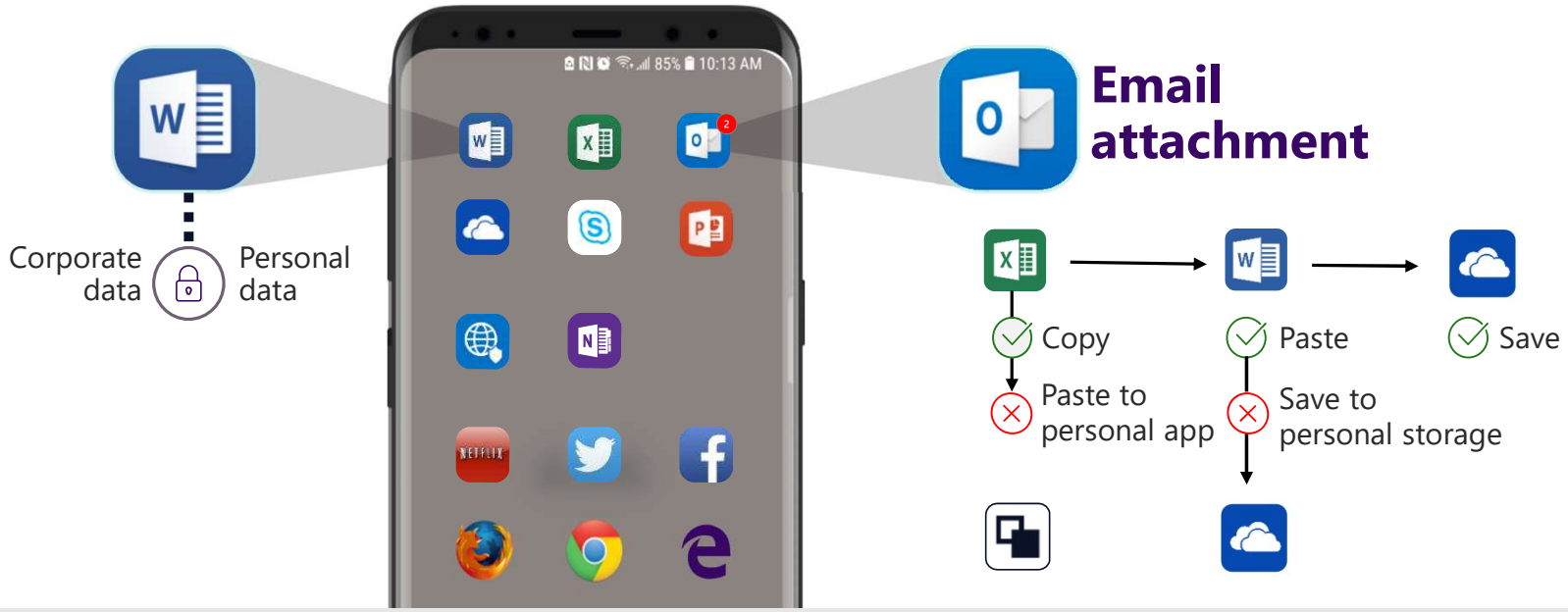


- Publish mobile apps to users
- Configure and update apps
- Report app inventory & usage
- Secure & remove corporate data within mobile apps

MICROSERVE

# Control what happens after data has been accessed

**Multi-identity policy**




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

Intune Azure AD

Allow
Enforce MFA
Enroll device

Block access
Wipe device

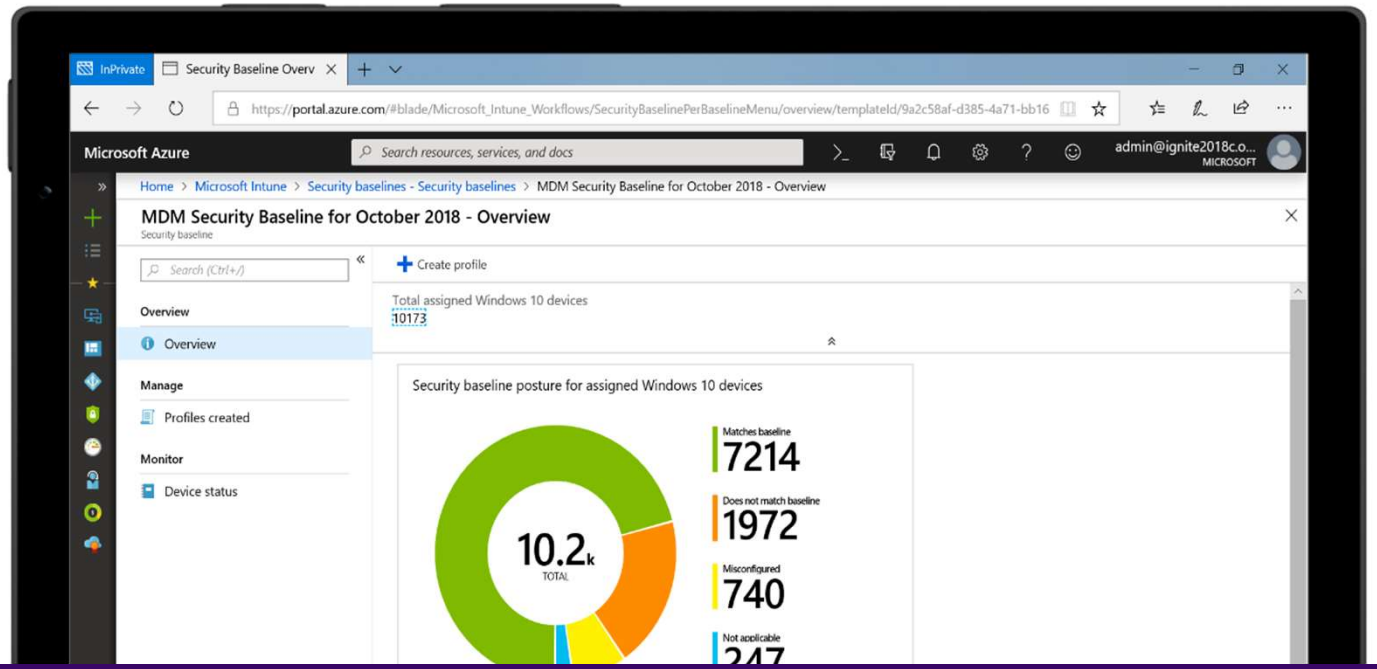
Office 365
Microsoft Azure

Microsoft Defender for Endpoint integration

Mobile threat defense (MTD) partners on iOS and Android

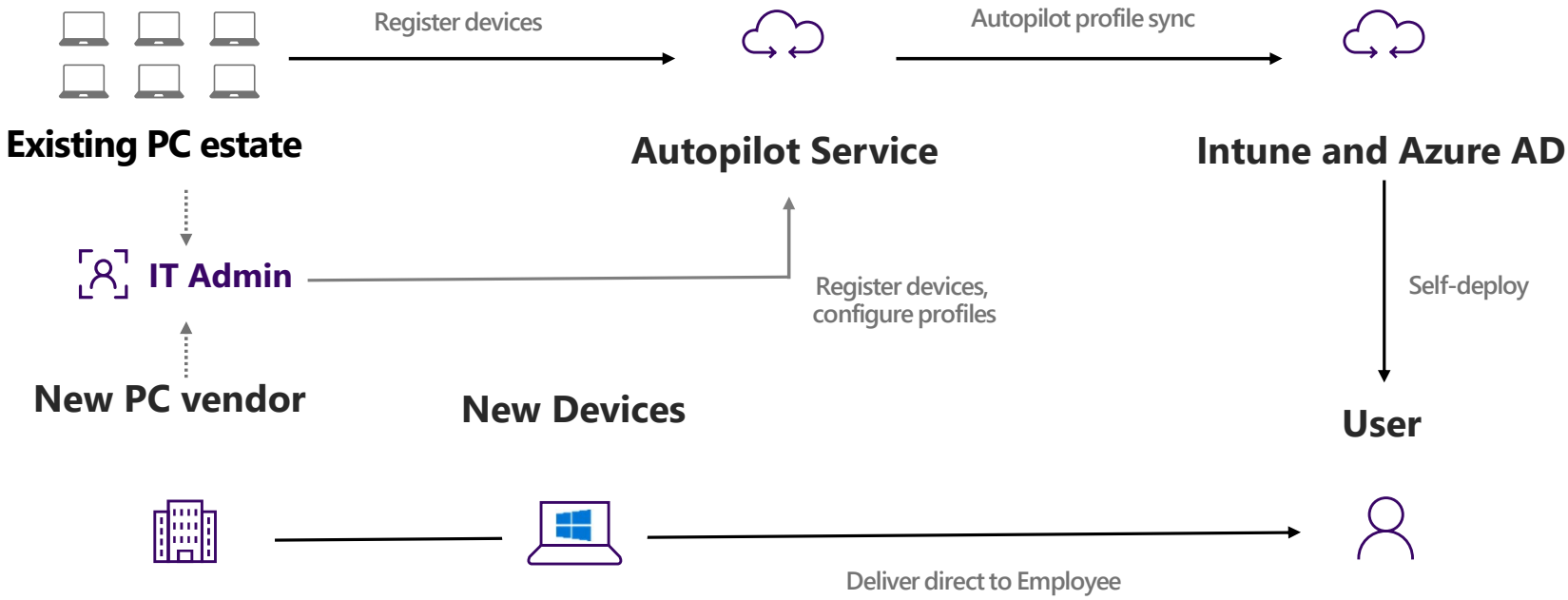
Microsoft · Lookout · Symantec · ZIMPERIUM · pradeo · Google Play Protect · Check Point

# Improve security posture with cloud-powered analytics



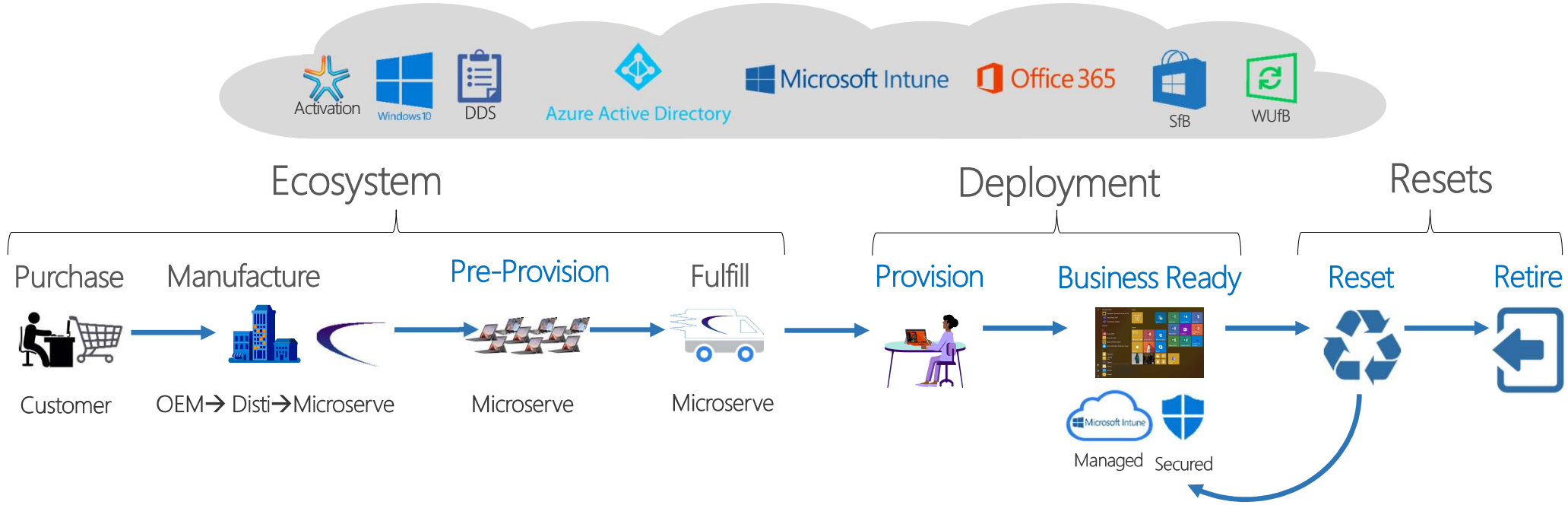

- Get insights from Microsoft cloud machine-learning
- Simplify migration to Intune policy settings using security baselines
- Monitor device compliance and automate remediation tasks

# 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

# Microserve Modern Deployment




Autopilot delivers zero touch **deployment & reset** experiences

MICROSERVE

# Endpoint Modernization Opportunity – how to get started

- ✓ Enable Hybrid AD
- ✓ Attach Intune to ConfigMgr ("Co-Management")
- ✓ Use Azure AD for SaaS app authentication
- ✓ Deploy MS Defender for Endpoint
- ✓ Manage & Secure meeting rooms

http://aka.ms/MicrosoftIgnite2020/MEM

MICROSERVE


# Q&A

Thank you for attending!


**VANCOUVER**
Unit 280
4400 Dominion Street
Burnaby, BC V5G 4G3
Tel: 604-473-9883

**CALGARY**
300-840 6th Ave SW
Calgary, AB T2P 3E5
Tel: 403-250-5888

**VICTORIA**
1969 Keating X Rd
Saanichton, BC V8M 2A4
Tel: 250-652-3737

**EDMONTON**
9657 45th Avenue
Edmonton, AB T6E 5Z8
Tel: 780-496-9585

**HALIFAX**
1701 Hollis Street
STE 800
Halifax, NS B3J 3M8
Tel: 902-580-5438

**www.microserve.ca**