Microsoft

Microsoft 365 Modern Desktop - Management

Sophie Chanialaki
Partner Technical Architect @ Microsoft CEE

What do we manage?

- Users (Identity, Access/Security)
- Devices (OS, Updates, Security)
- Data (Access/Security)
- Applications (Access/Security)

Management Choices

Traditional Management

- Works with existing infrastructure
- Continued support for Group Policy and WMI

Modern Management

- Advanced MDM support
- Consistent across PC/phone
- 1st and 3rd party solutions

Available Choices	
Identity	▪ Active Directory ▪ Azure Active Directory
Management	▪ Group Policy ▪ System Center Configuration Manager ▪ 3rd Party Infrastructure Management ▪ Microsoft Intune ▪ 3rd Party MDM
Updates & Upgrades	▪ Windows Update ▪ Windows Server Update Services ▪ Software Update Point (System Center Configuration Manager) ▪ Microsoft Intune ▪ 3rd Party MDM
Infrastructure	▪ On Premises ▪ Cloud
Ownership	▪ Corporate Owned ▪ Choose Your Own Device (CYOD) ▪ Bring Your Own Device (BYOD)

Identity and Access Management

The Current Reality

HIGHTAIL Dropbox amazon web services Microsoft Azure EC2 Microsoft Dynamics box CONCUR Basecamp

ShareFile by CITRIX GoToMeeting by CITRIX salesforce.com force.com Office 365 SAP SUGARCRM Microsoft System Center

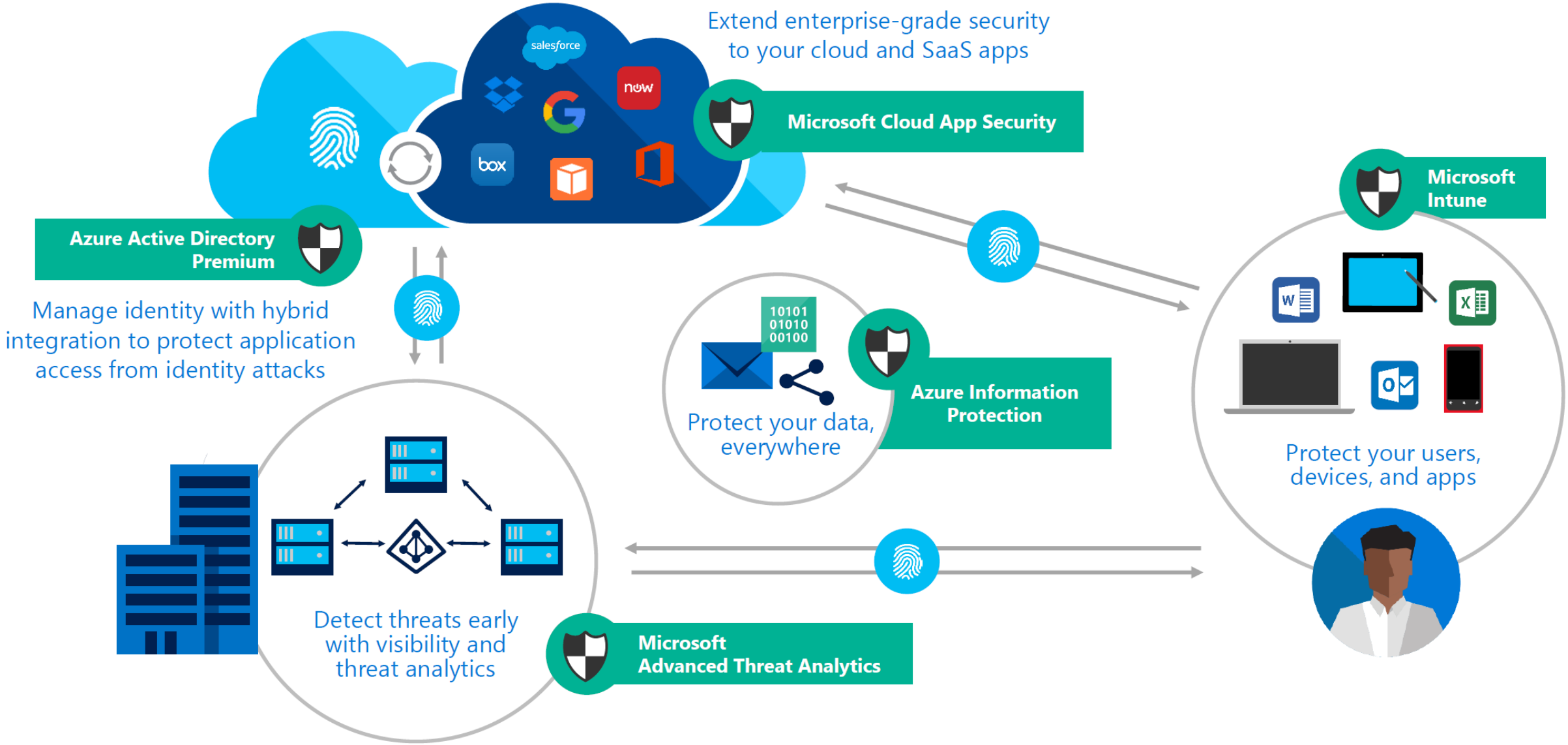
On-premises

Managed devices

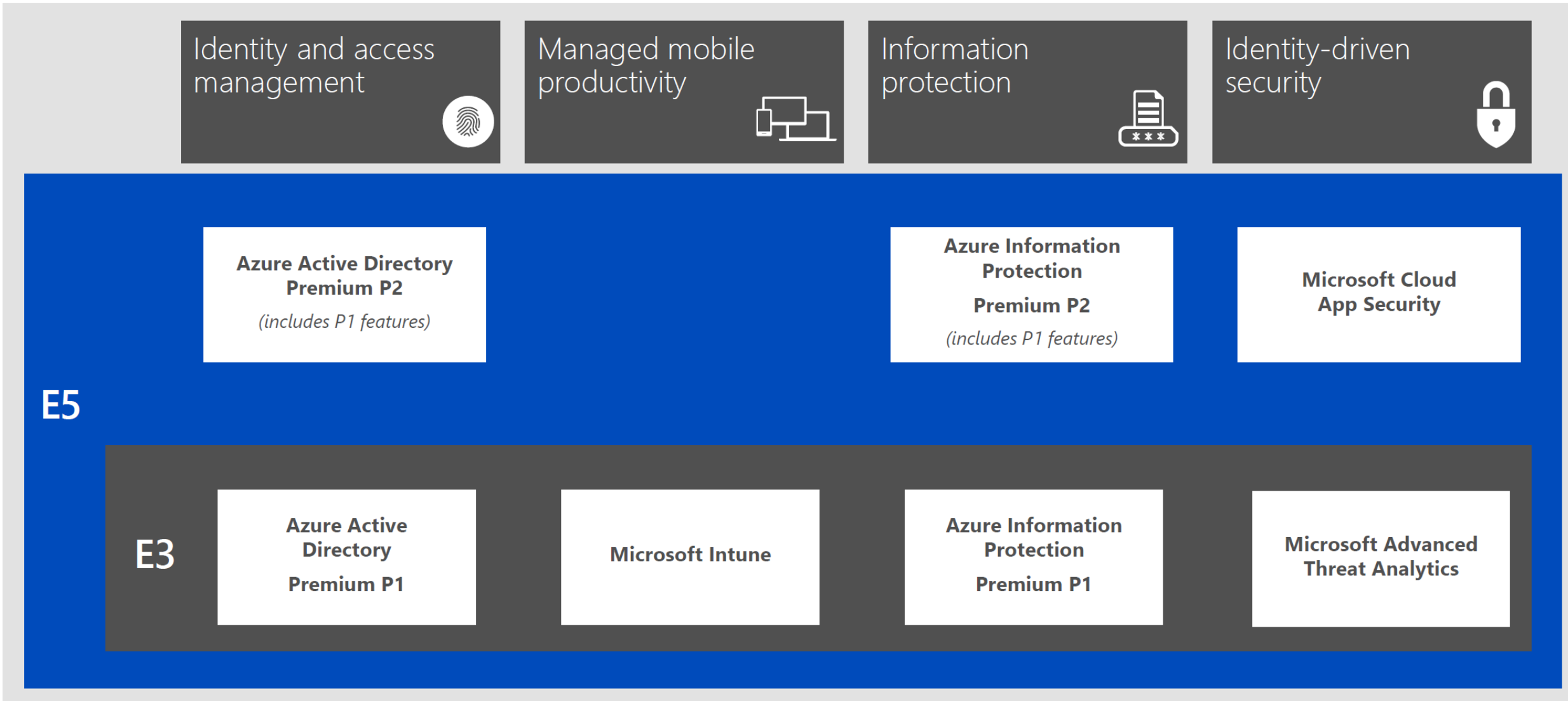
Active Directory

Windows Server

Enterprise Mobility +Security



Enterprise Mobility + Security packaging

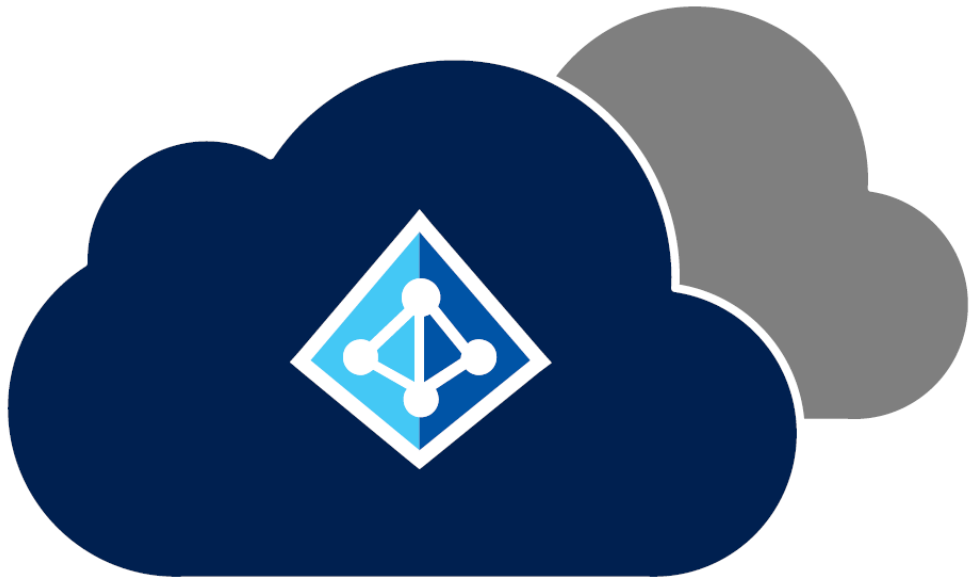


Azure Active Directory Premium

What is Azure Active Directory

A comprehensive identity and access management cloud solution for your employees, partners, and customers.

It combines directory services, advanced identity governance, application access management, and a rich standards-based platform for developers.

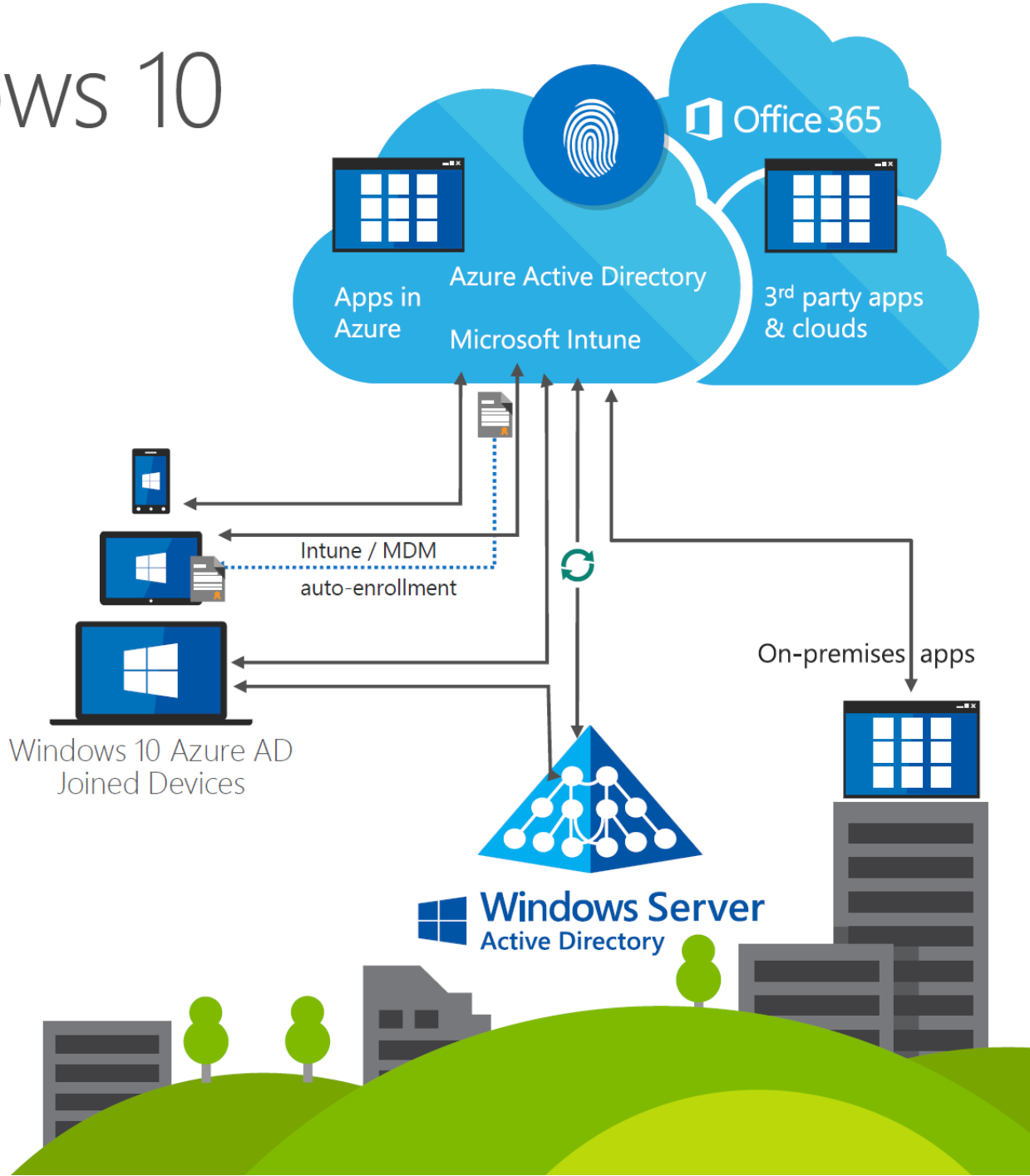


Azure AD Join for Windows 10

Azure AD Join makes it possible to connect work-owned Windows 10 devices to your company's Azure Active Directory.

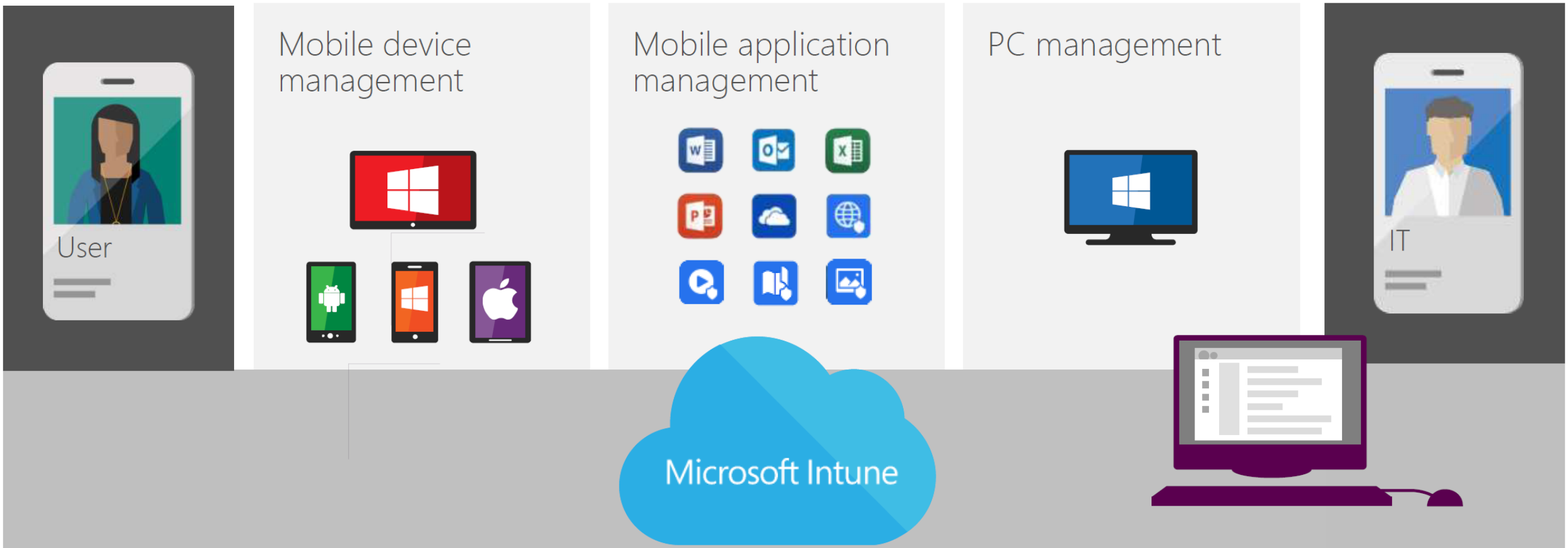
With Azure AD Join, you can auto enroll devices in Microsoft Intune for management.

- Intune auto-enrollment
- Enterprise-compliant services
- Single sign-on from the desktop to cloud and on-premises applications with no VPN
- Support for hybrid environments

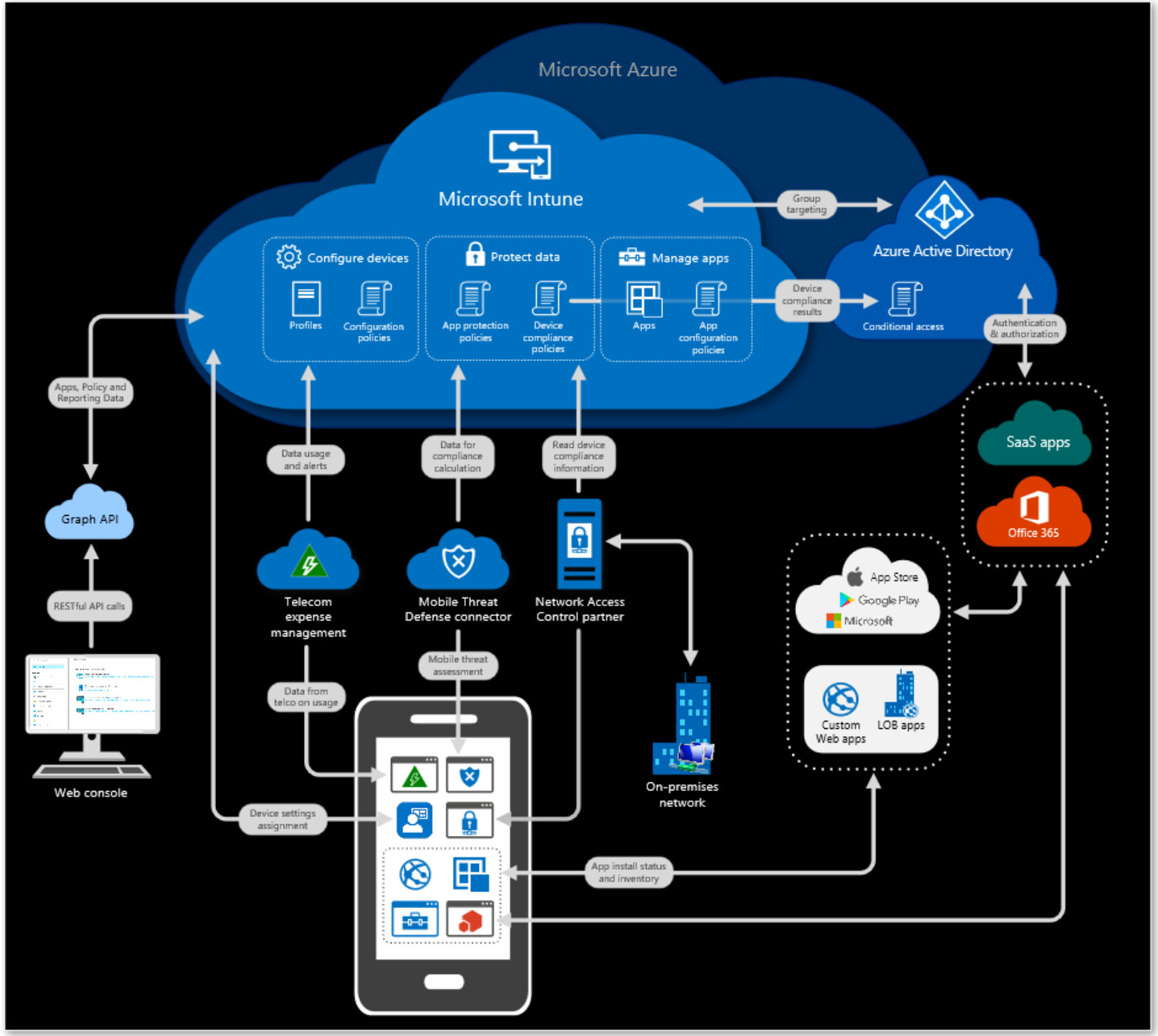


Intune

Enterprise mobility management with Intune



Intune helps organizations provide their employees with access to corporate applications, data, and resources from virtually anywhere on almost any device, while helping to keep corporate information secure.


Microsoft Azure
Microsoft Intune
Configure devices
Profiles
Configuration policies
Protect data
App protection policies
Device compliance policies
Manage apps
Apps
App configuration policies
Group targeting
Azure Active Directory
Device compliance results
Conditional access
Authentication & authorization
Apps, Policy and Reporting Data
Graph API
RESTful API calls
Web console
Data usage and alerts
Data for compliance calculation
Read device compliance information
Telecom expense management
Mobile Threat Defense connector
Network Access Control partner
Mobile threat assessment
Data from telco on usage
Device settings assignment
On-premises network
SaaS apps
Office 365
App Store
Google Play
Microsoft
Custom Web apps
LOB apps
App install status and inventory

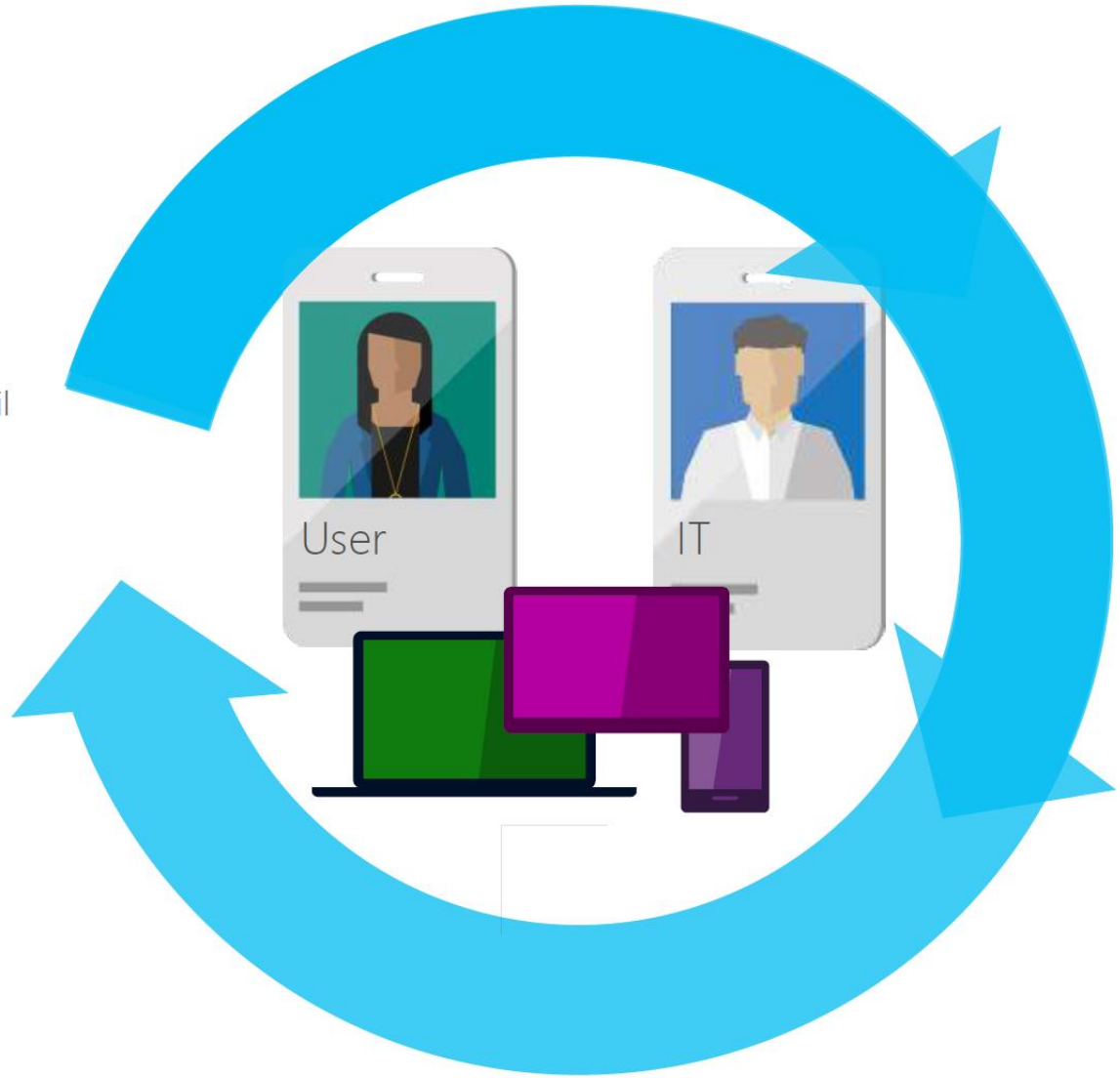
Comprehensive lifecycle management

Enroll

- Provide a self-service Company Portal for users to enroll devices
- Deliver custom terms and conditions at enrollment
- Bulk enroll devices using Apple Configurator or service account
- Restrict access to Exchange email if a device is not enrolled

Provision

- Deploy certificates, email, VPN, and WiFi profiles
- Deploy device security policy settings
- Install mandatory apps
- Deploy app restriction policies
- Deploy data protection policies



Retire

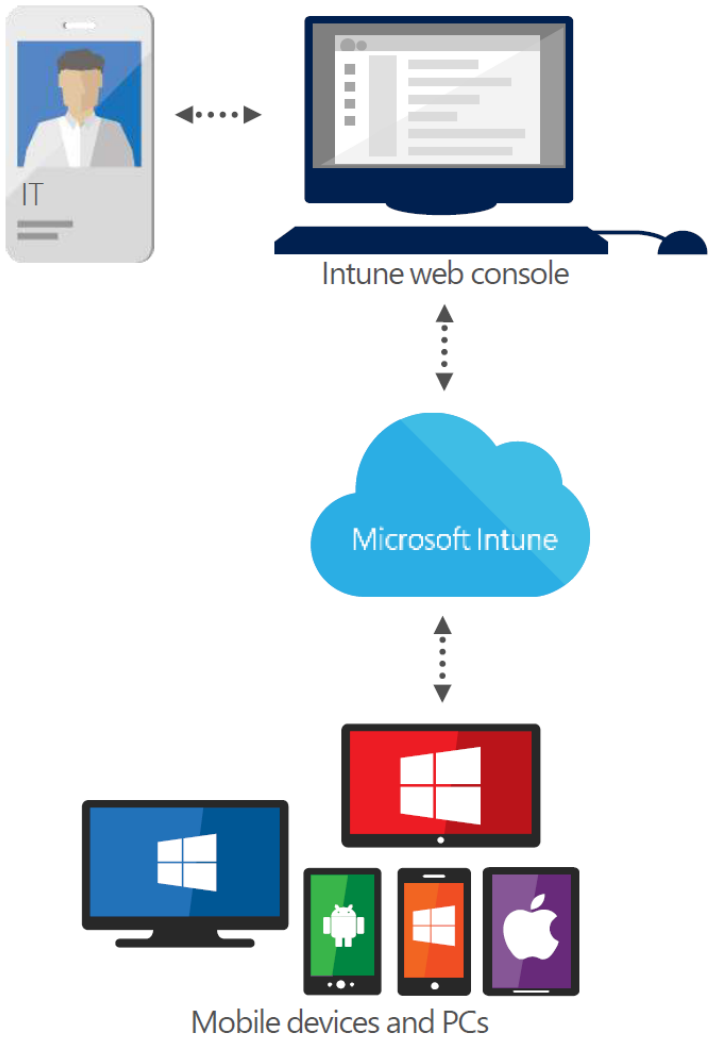
- Revoke access to corporate resources
- Perform selective wipe
- Audit lost and stolen devices

Manage and Protect

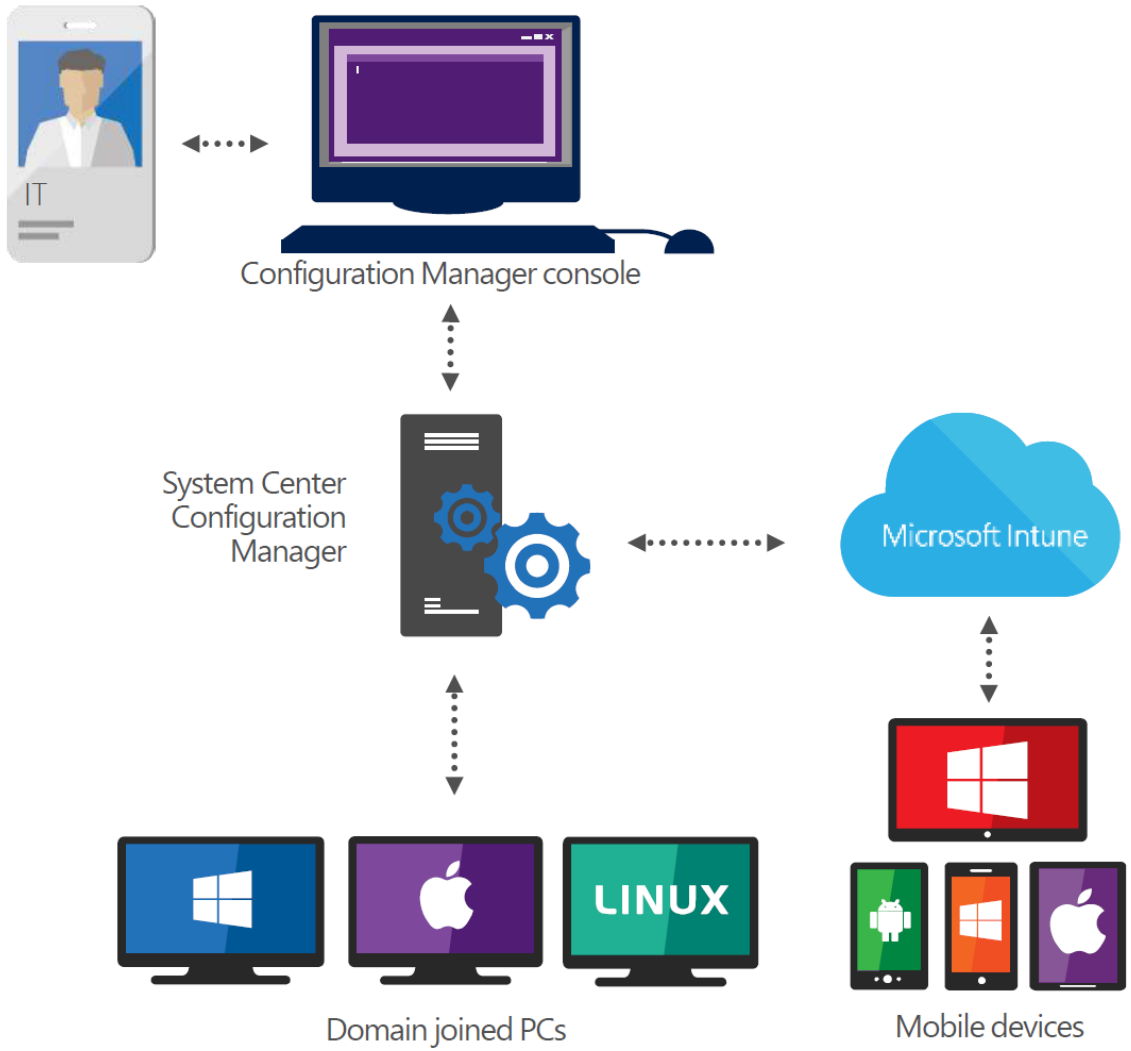
- Restrict access to corporate resources if policies are violated (e.g., jailbroken device)
- Protect corporate data by restricting actions such as copy, cut, paste, and save as between Intune-managed apps and personal apps
- Report on device and app compliance

Deployment flexibility

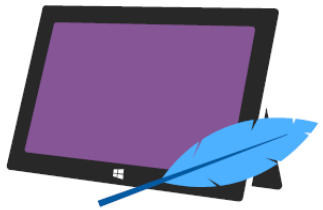
Intune standalone (cloud only)



Configuration Manager integrated with Intune (hybrid)



PC management



Intune standalone (cloud only)	Configuration Manager integrated with Intune (hybrid)
Lightweight, agentless OR agent-based management	Agent-based management only
PC protection from malware	PC protection from malware
PC software update management	PC software update management
Software distribution	Software distribution
Proactive monitoring and alerts	Proactive monitoring and alerts
Hardware and software inventory	Hardware and software inventory
Policies for Windows Firewall management	Policies for Windows Firewall management
	Operating system deployment
	PC, mobile device, Windows Server, Linux/Unix, Mac, and virtual desktop management
	Power management
	Custom reporting

MDM Intune Policy Options

Configuration policies	▪ These are commonly used to manage security settings and features on your devices ▪ Examples include password, encryption, hardware, system, features, etc.
Device compliance policies	▪ Compliance policies are used with conditional access policies to allow only devices that comply with compliance policy rules to access email and other services ▪ Examples include PIN or password, email profile, minimum OS version, and Windows health attestation
Conditional access polices	▪ Conditional access policies are set to conditional access policy to restrict access ▪ Examples include device compliance status, the platform running on the device, and the type of apps used to access the services
Corporate device enrollment policies	▪ Microsoft from virtually anywhere on almost any device, while helping to keep corporate information secure
Resource access policies	▪ Microsoft Intune Wi-Fi, VPN, and email profiles work together to help your users gain access to the files and resources that they need to do their work wherever they are. Certificate profiles help secure that access

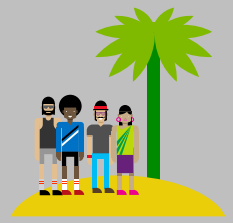
Dynamic Management

Overview	Windows 10 allows you to manage devices differently depending on location, network, or time. Settings will be enforced even if the device can't reach the management server when the location or network changes.
Example	Managed devices can have cameras disabled when at a work location, the cellular service can be disabled when outside the country to avoid roaming charges, or the wireless network can be disabled when the device is not within the corporate building or campus.
Configurations	▪ Geolocation, Network and Time Based triggers ▪ Policy Configuration and enforcement is local to the device ▪ Policies are applied offline ▪ Support both enable and disable by default

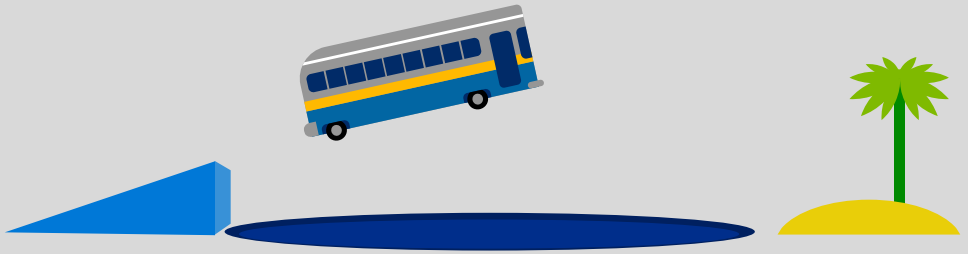
Transition to Co-Management/Modern

Paths to Modern Management

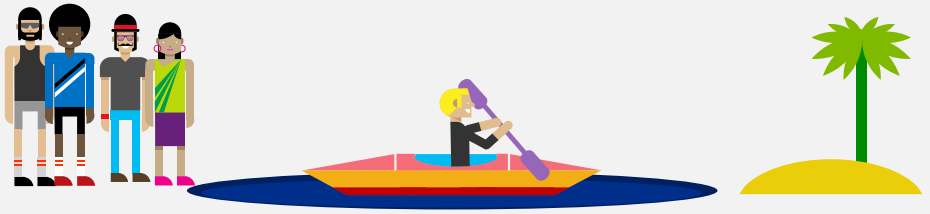
Cloud-first



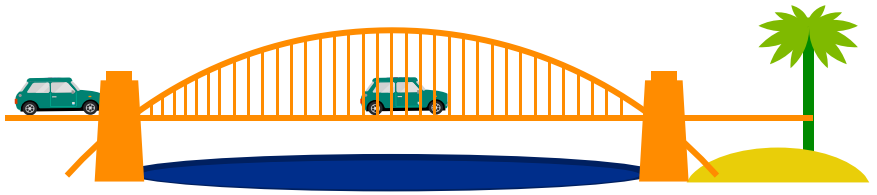
Big Switch Transition



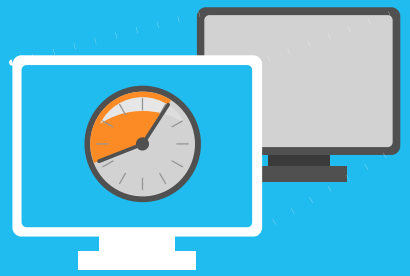
Group by Group Transition



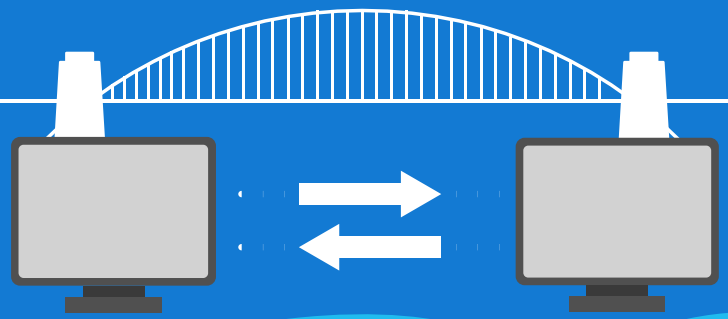
Iterative (“Co-management”)



Co-Management



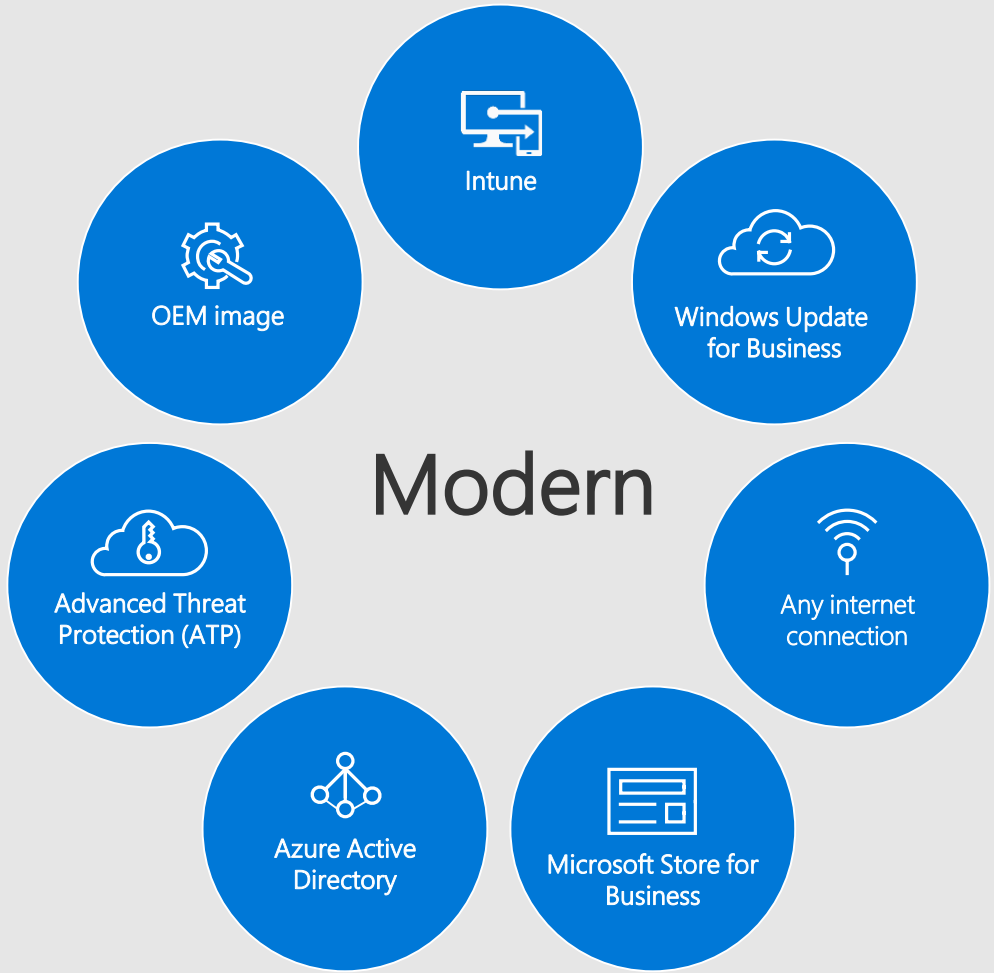
A practical way to migrate over time



Modern is not “all or nothing”

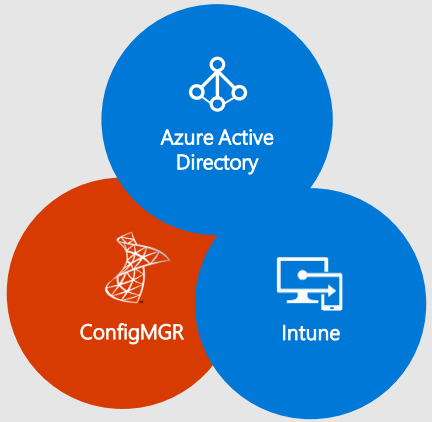
Minimize risk

Revolution

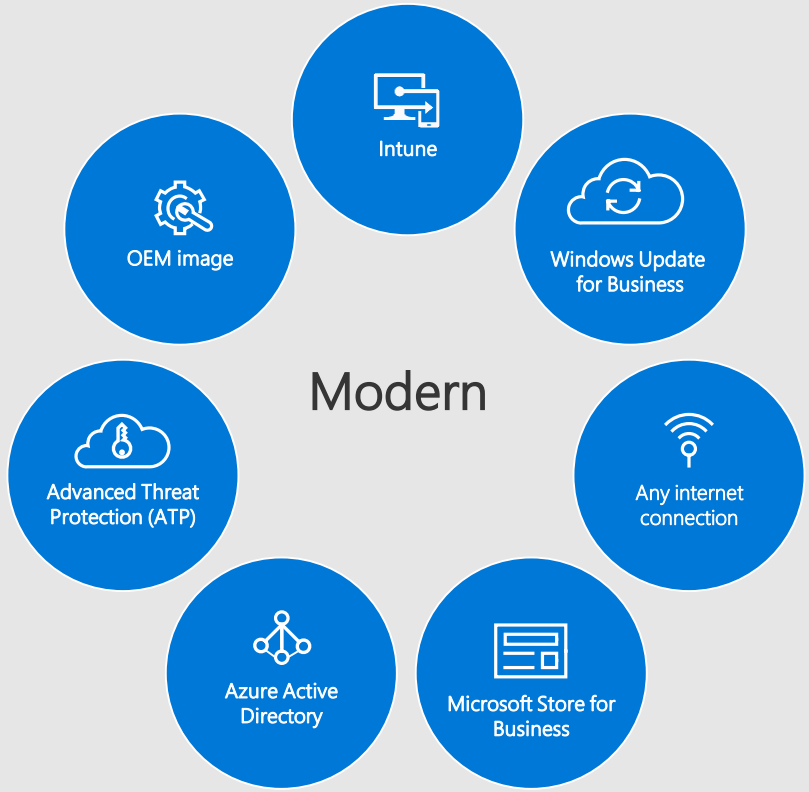


Evolution

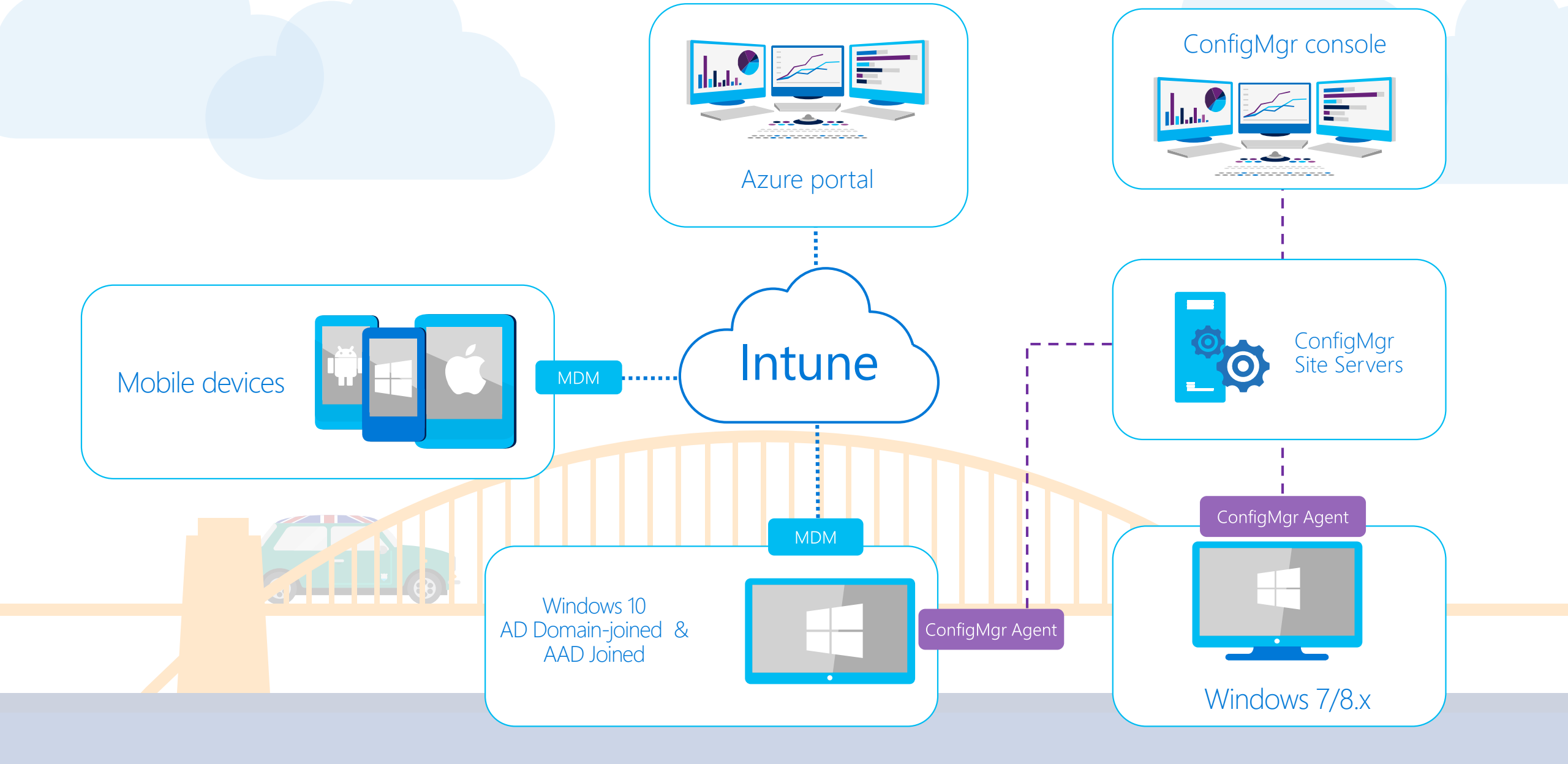
Co-management



- Allows organizations to take a first step toward Modern Management to build confidence and momentum
- Intune is primary management solution
- ConfigMGR is available as contingency



Co-Management Architecture With ConfigMgr and Intune



Bridging to Modern Management