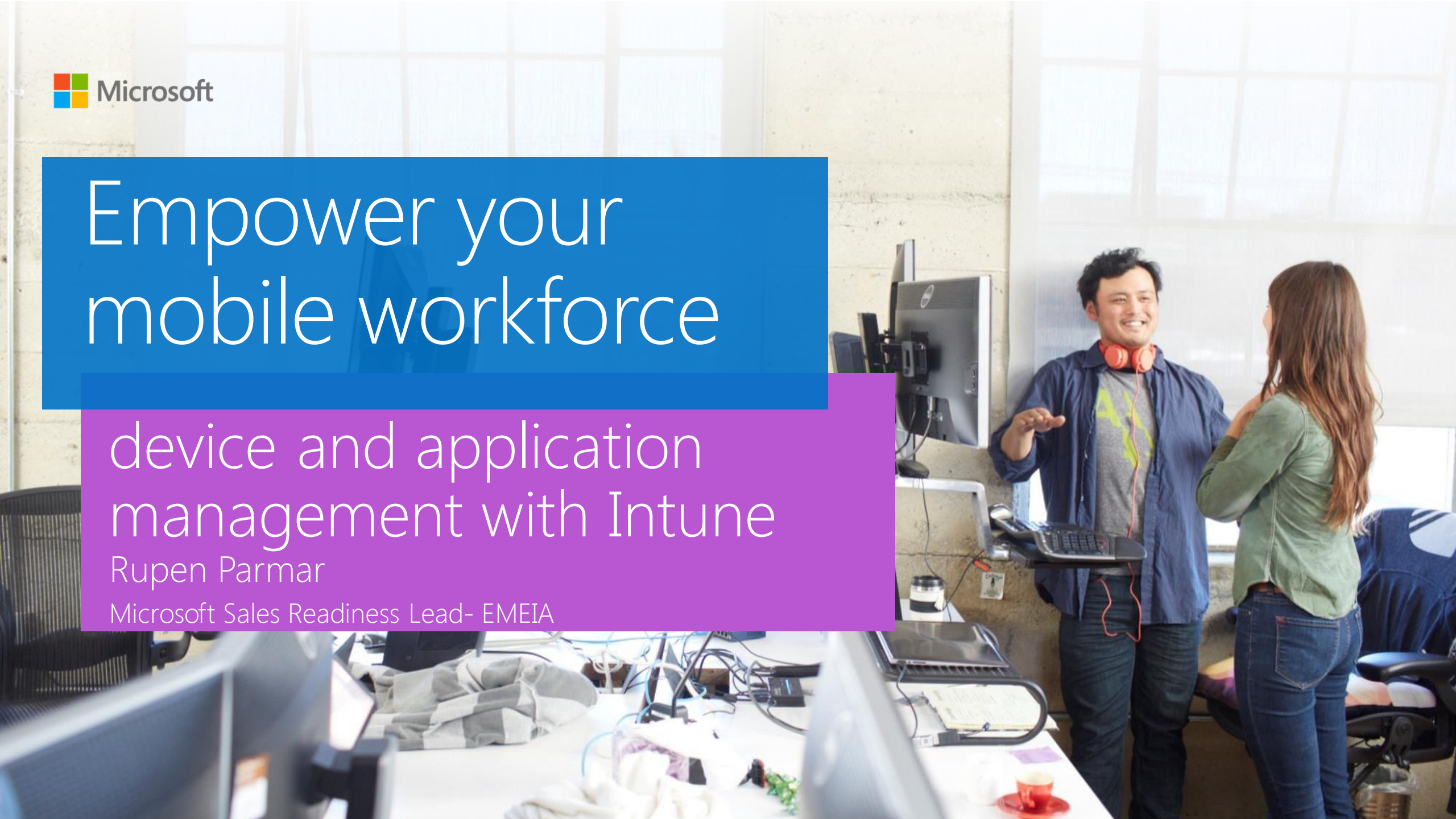
Microsoft

Empower your mobile workforce

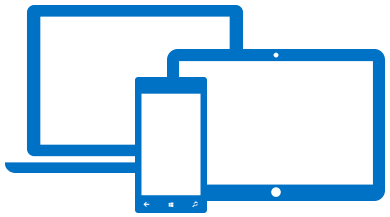
device and application management with Intune

Rupen Parmar

Microsoft Sales Readiness Lead- EMEIA



Business mobility is changing
Mobility management and security is top of mind



52% of employees across 17 countries report using **3** or more devices for work.

74% of companies allow BYOD usage at work. **66%** of employees use personal devices at work.

80% of employees use unapproved apps at work. **93%** of employees admitted violating information security polices.

Security is the **#1 concern** for CIOs in 2015 with **45%** increase in security incidents in 2014

50% of companies have experienced a data breach due to device security

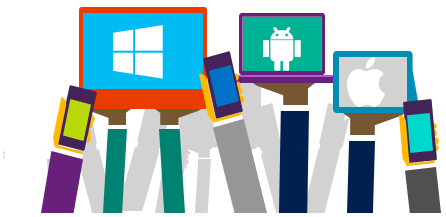
30% of all cyber attacks were **targeted at SMBs** in 2014.

Cyber crime costs SMBs nearly **4X cost of larger firms.**

Average time to contain a cyber attack is **30 days.**.

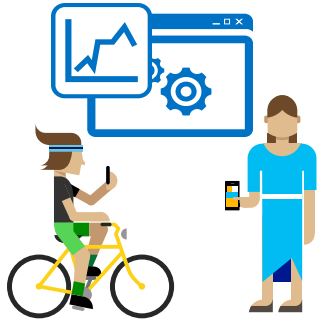
Microsoft

What this means for companies
Empowering productivity and protecting corporate assets



personal devices

Drive productivity and satisfaction with BYOD.



secure access

Provide secure access to corporate data and resources

remote offices

Deploy and manage devices remotely.

reduce costs

Simplify management. Reduce costs.

So how do you protect your business assets while keeping your mobile workers happy and productive?

Microsoft Intune

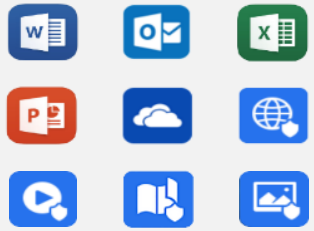
Empowering productivity. Simplifying Management.

Mobile device management

- BYOD, CYOD
- Windows, iOS, Android
- Per user licensing

+

Mobile application management



- Office 365
- Line-of-business apps (SaaS)

+

PC management

- Windows 8.1 and Mac computers
- Integration with System Center

=

Microsoft Intune
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 Wi-Fi 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

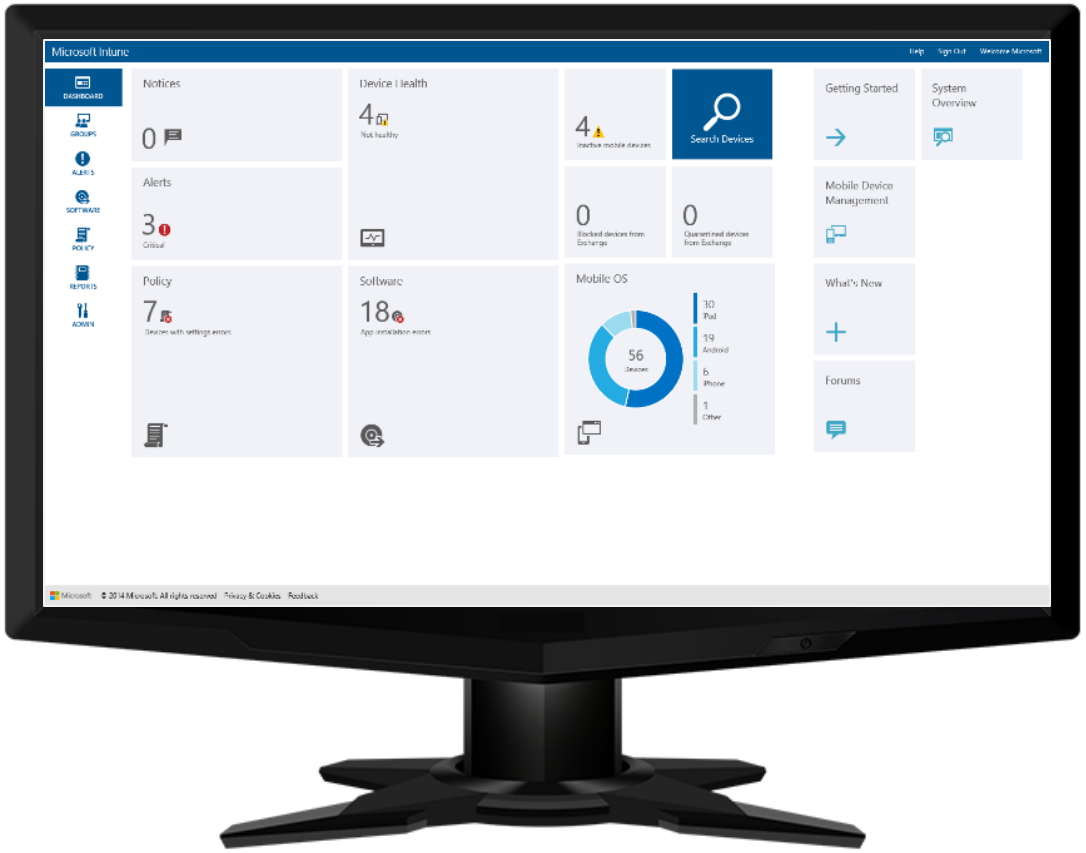
- Restrict access to corporate resources if policies are violated (e.g., jailbroken device)
- Protect corporate data by restricting actions such as copy/cut/paste/save outside of managed app ecosystem
- Report on device and app compliance

Microsoft

Microsoft Intune

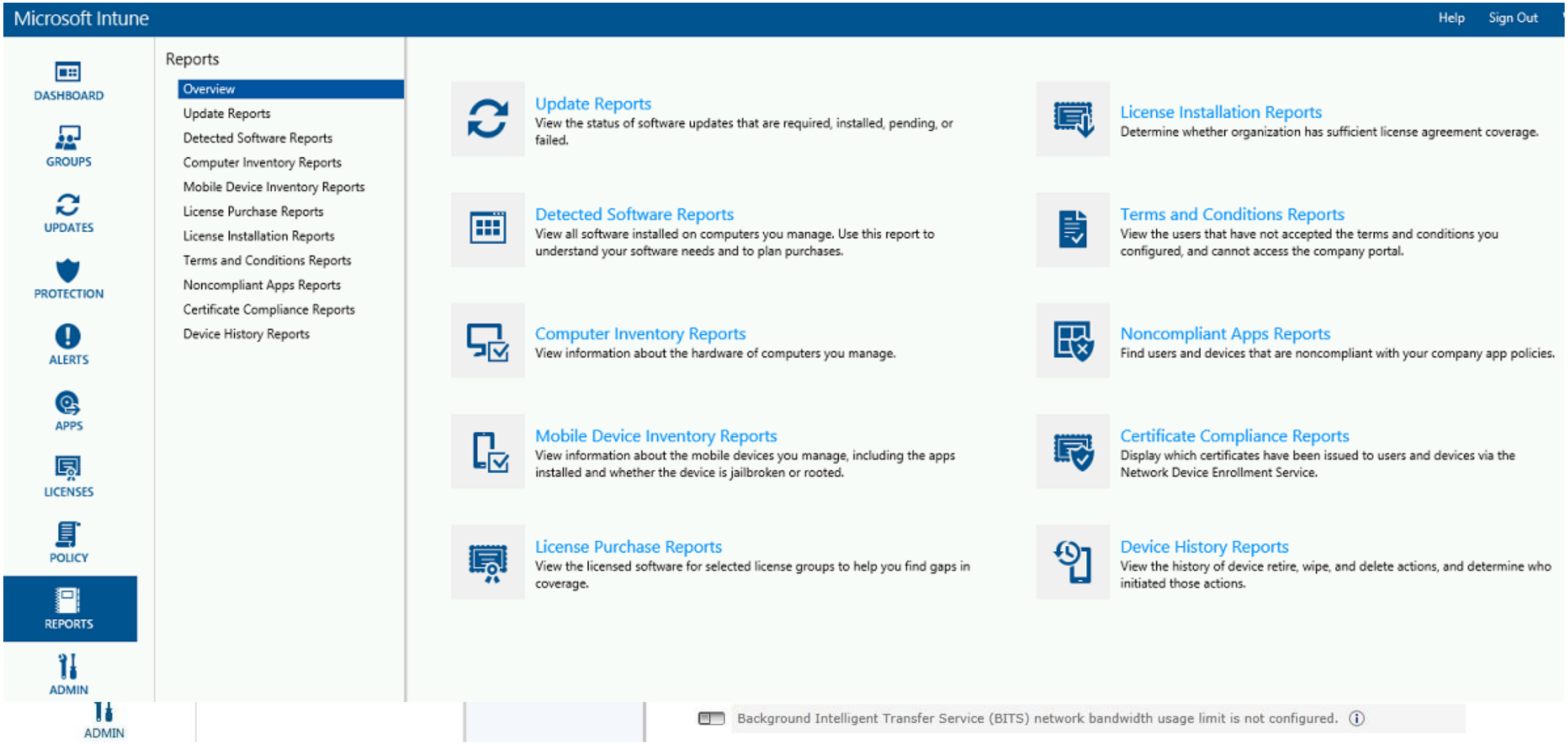
Single management console for IT admins

- Intuitive dashboard
- Respond to alerts
- Manage software deployments
- Configure and deploy policies
- View reports
- Role-based management



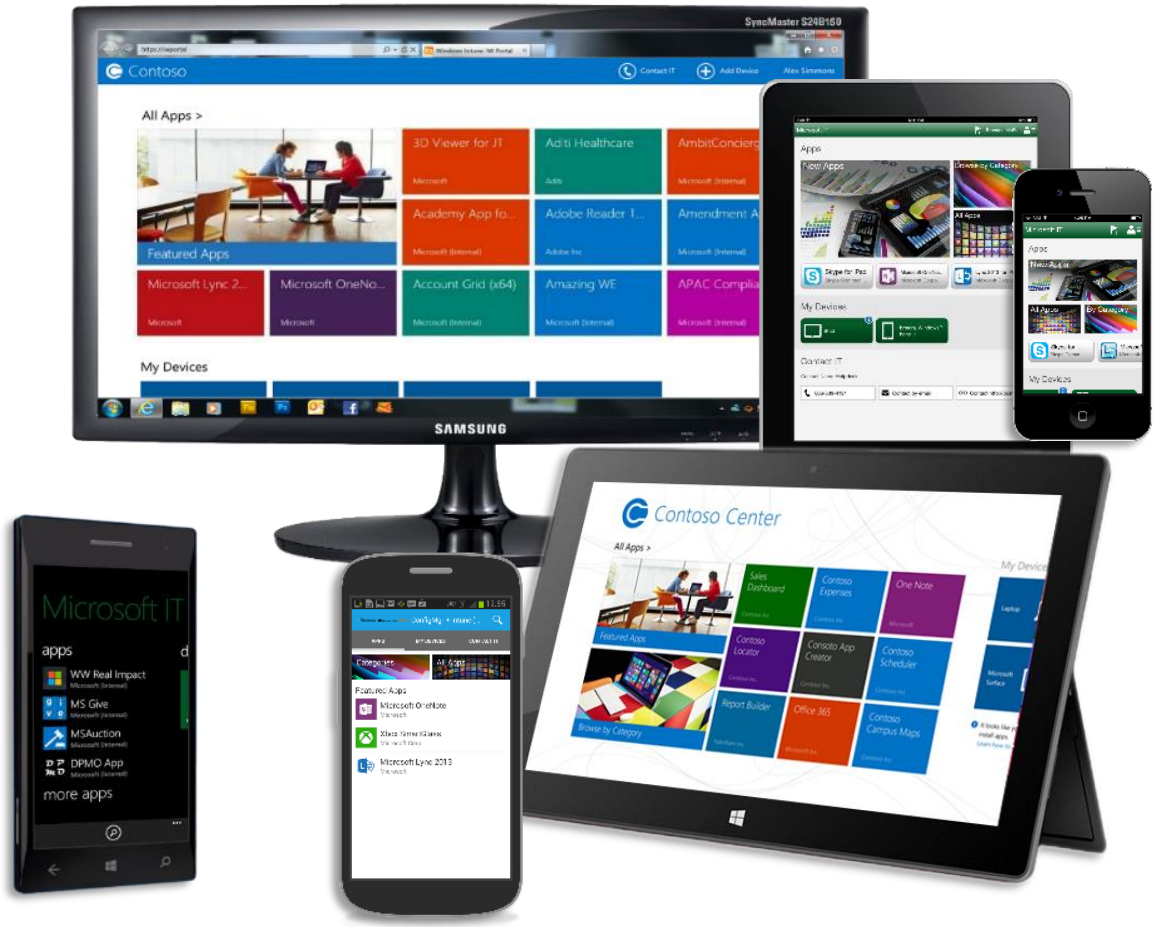
Microsoft

Single management console for IT admins



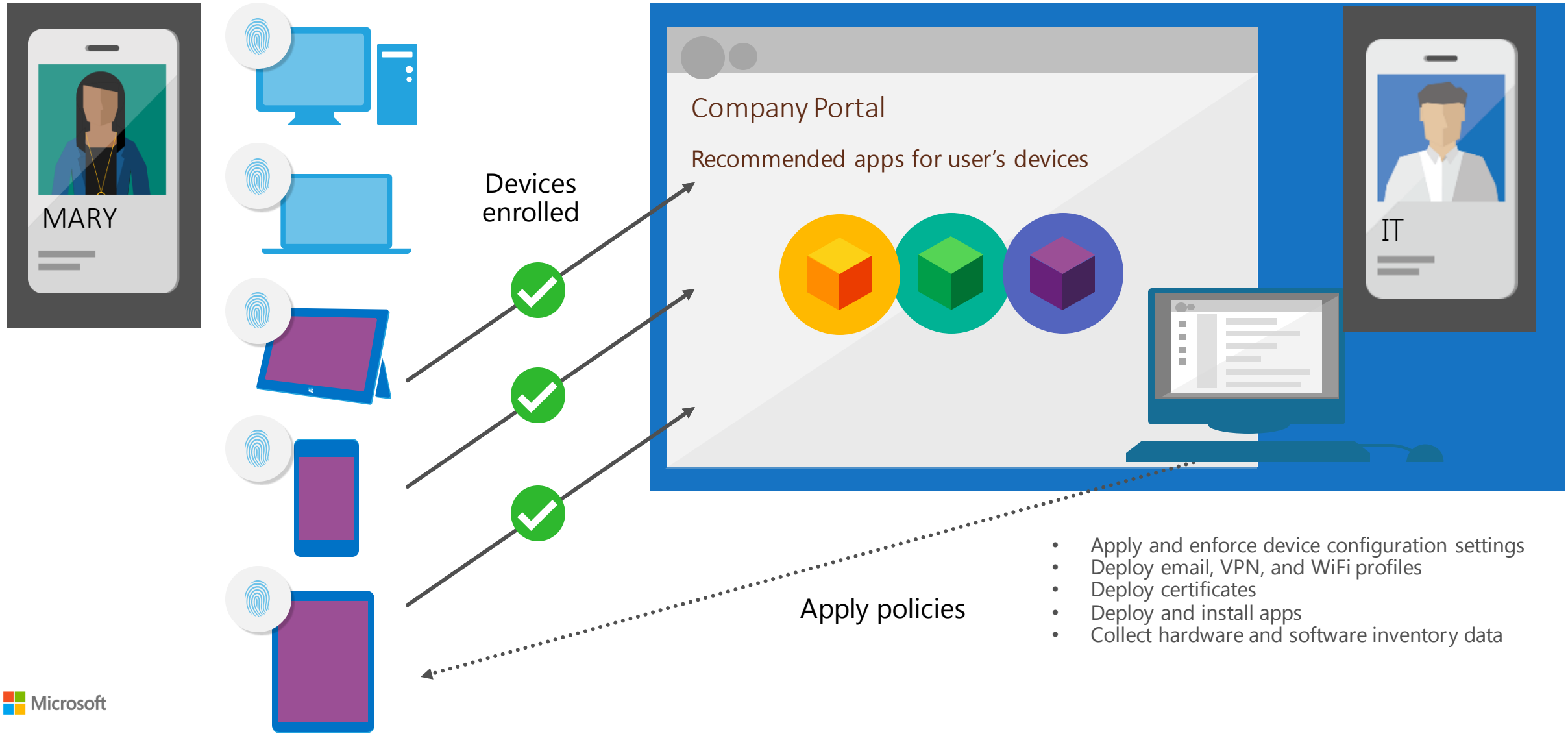
Microsoft Intune
Self-service company portal

- Consistent experience across devices
- Manage devices and data
- Install corporate applications
- Contact IT
- Customizable terms and conditions



Microsoft Intune

Mobile device management

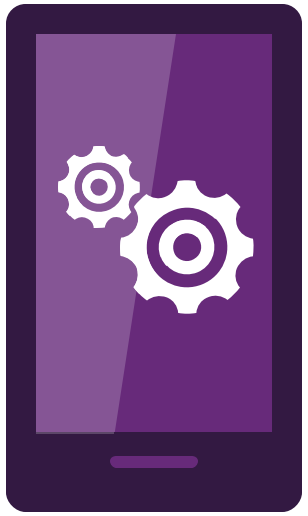


Microsoft

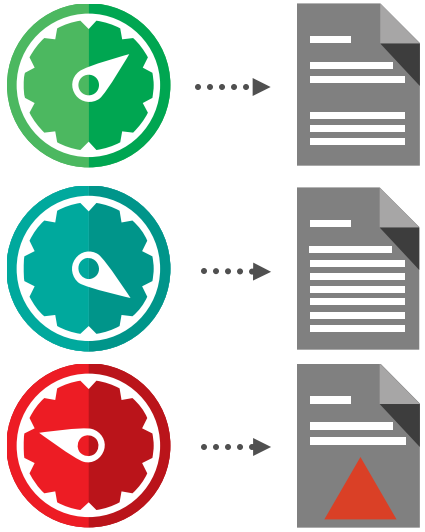
Microsoft Intune

Device settings management

Comprehensive security policies are enforced on each platform



Extensive configuration settings are available for each platform

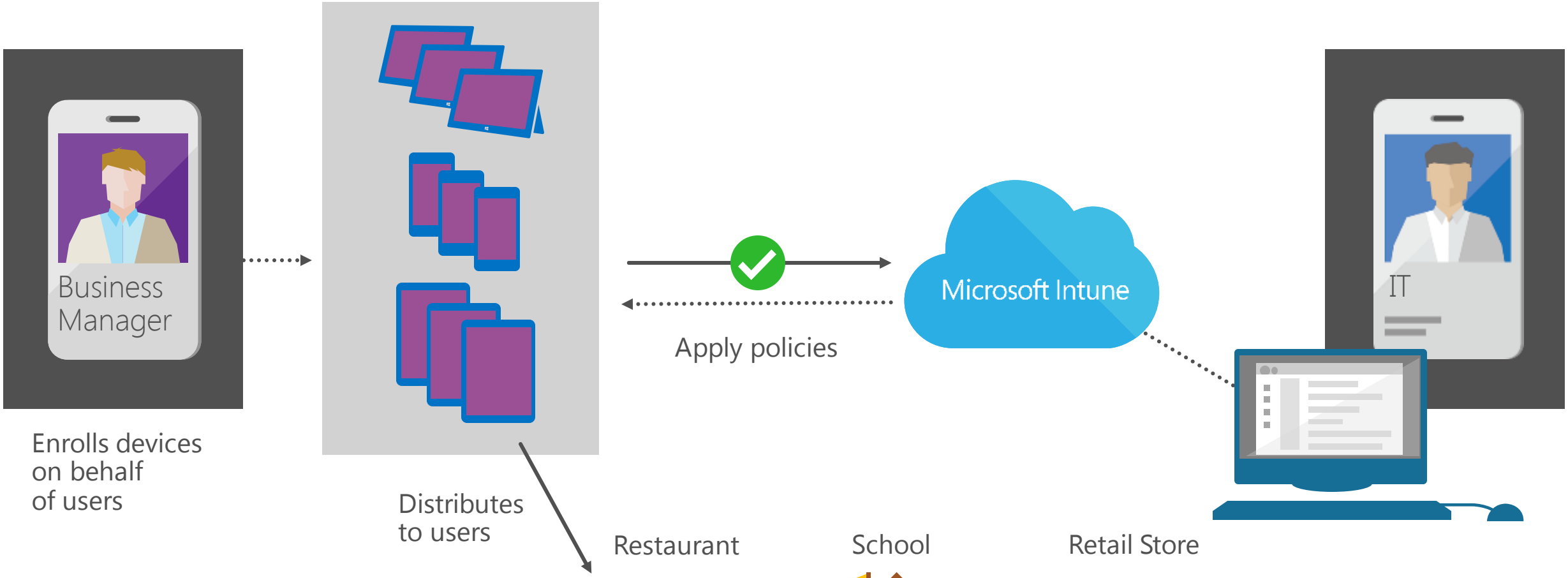


Reporting available on each setting whether it is applicable, conformant or has an error

Policies can be applied to user and device groups

Microsoft Intune

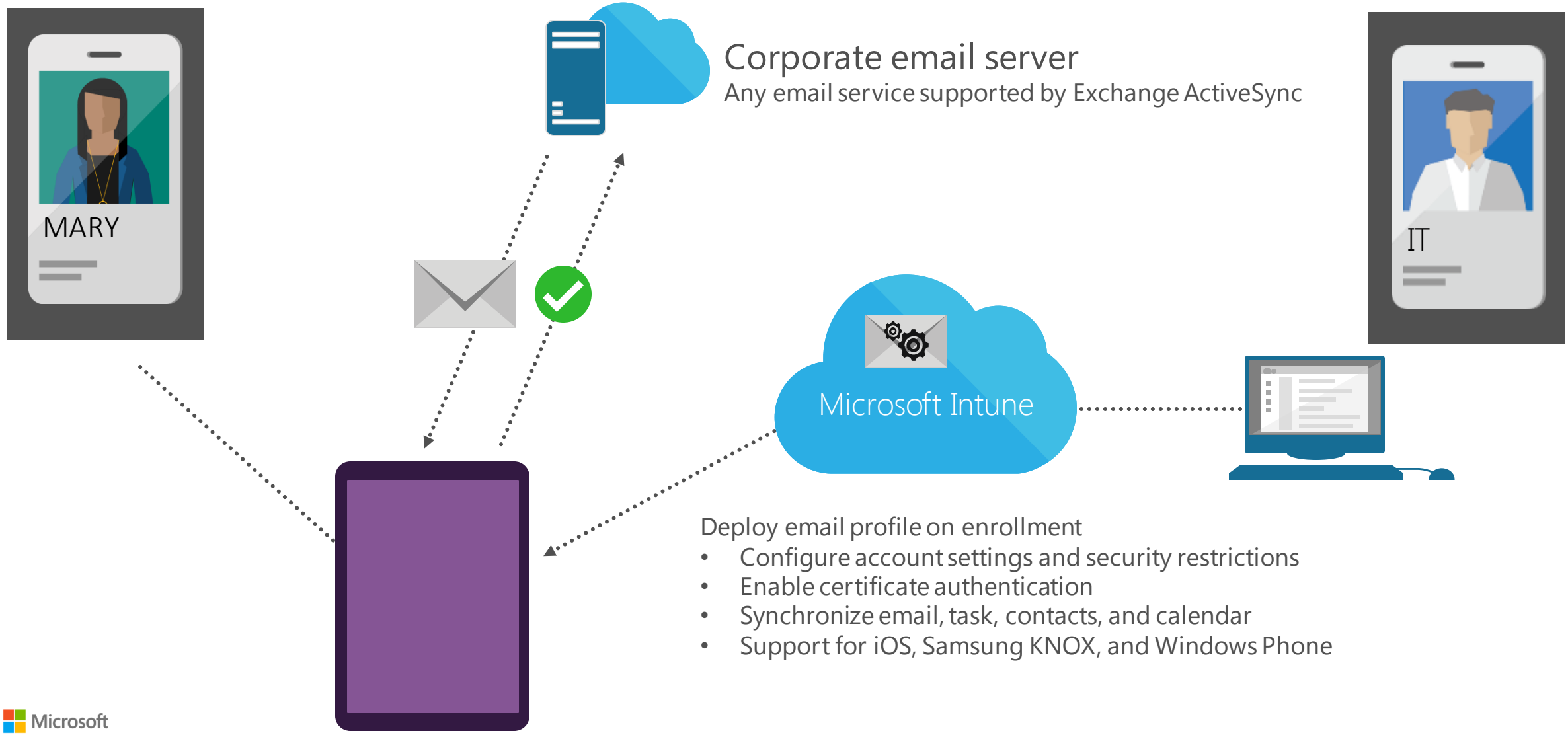
Bulk enrollment of up to 1,000 devices



Microsoft

Microsoft Intune

Email profile management



Deploy email profile on enrollment

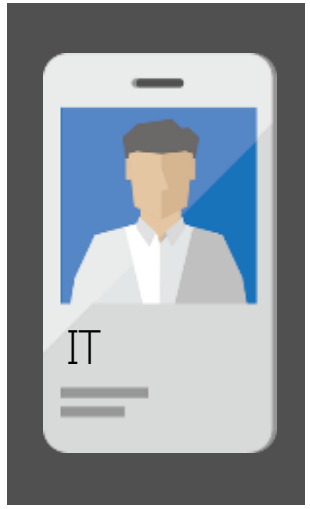
- Configure account settings and security restrictions
- Enable certificate authentication
- Synchronize email, task, contacts, and calendar
- Support for iOS, Samsung KNOX, and Windows Phone

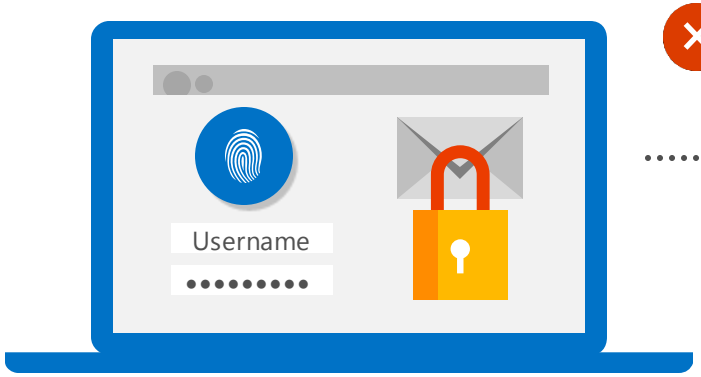
Microsoft Intune

Conditional access to email

Required settings defined by IT admin:

- Enrolled device
- Encrypted device
- Passcode set
- Not jailbroken/rooted



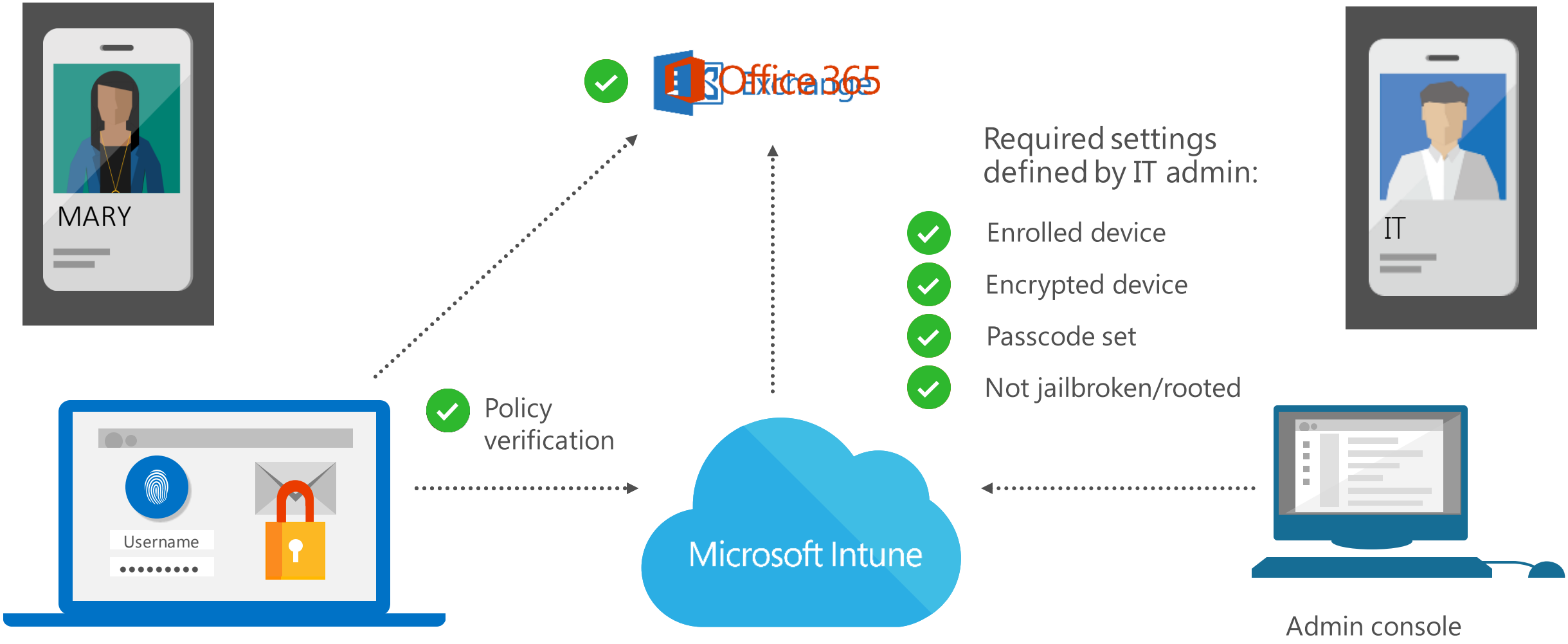


Policy verification

Admin console

Microsoft Intune

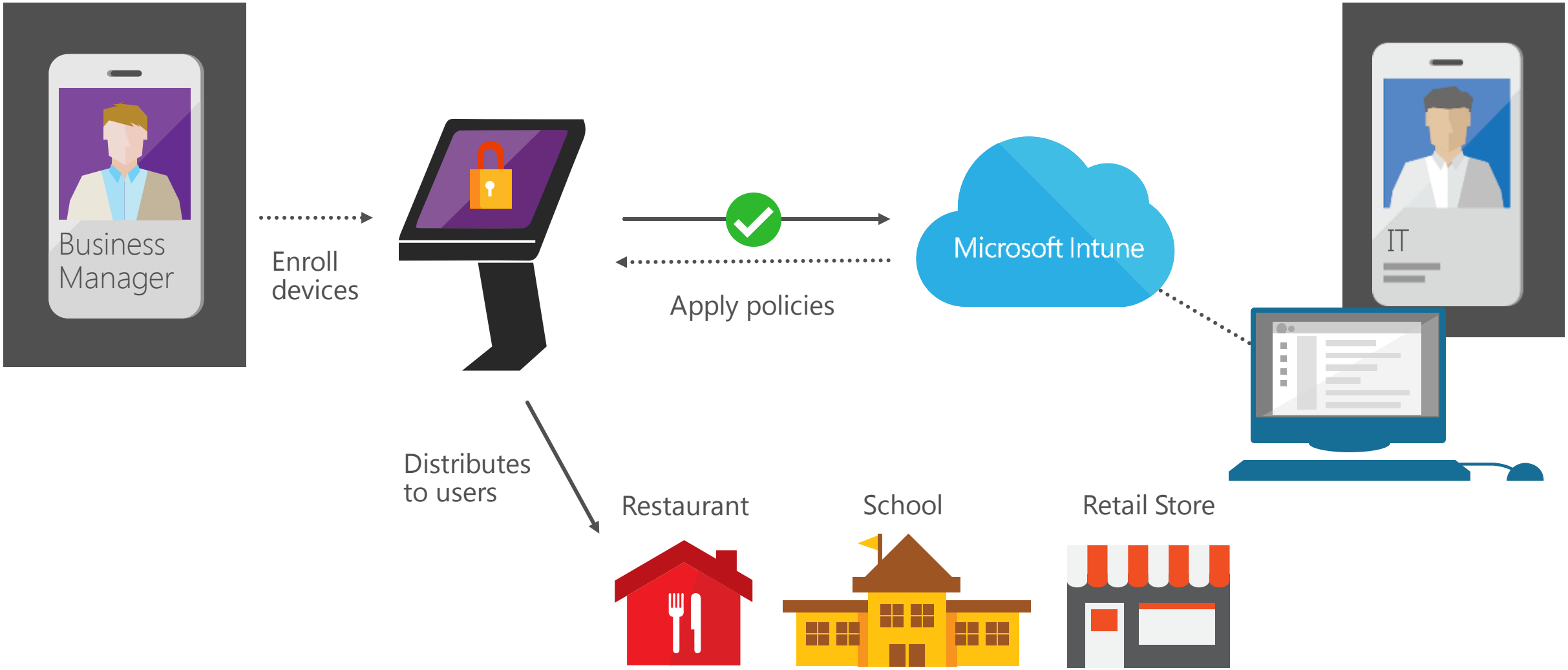
Conditional access to email



Microsoft

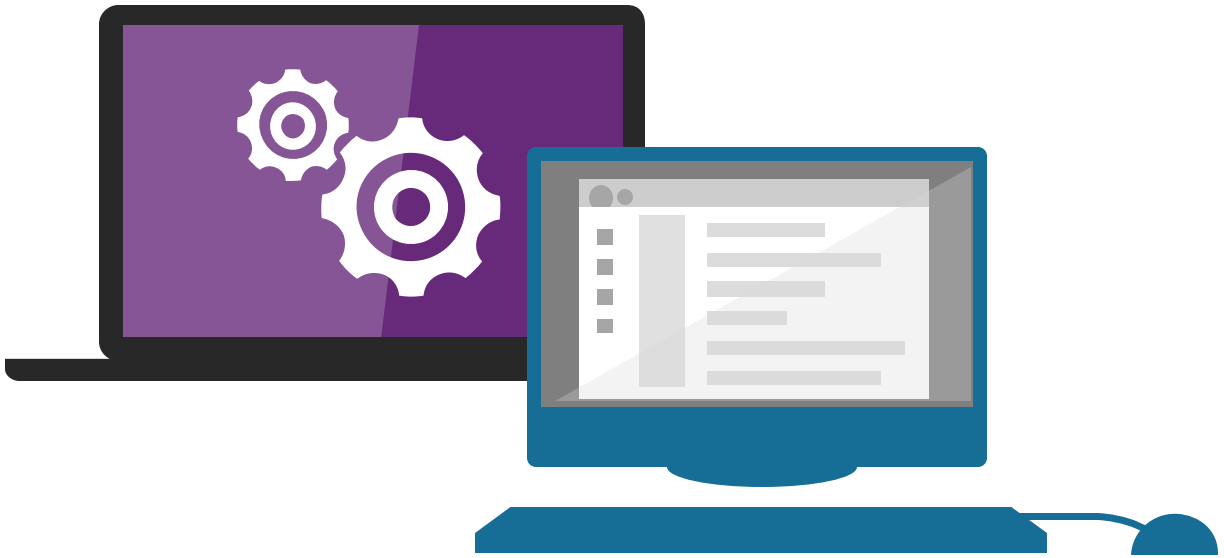
Microsoft Intune

Device lock down



Microsoft Intune

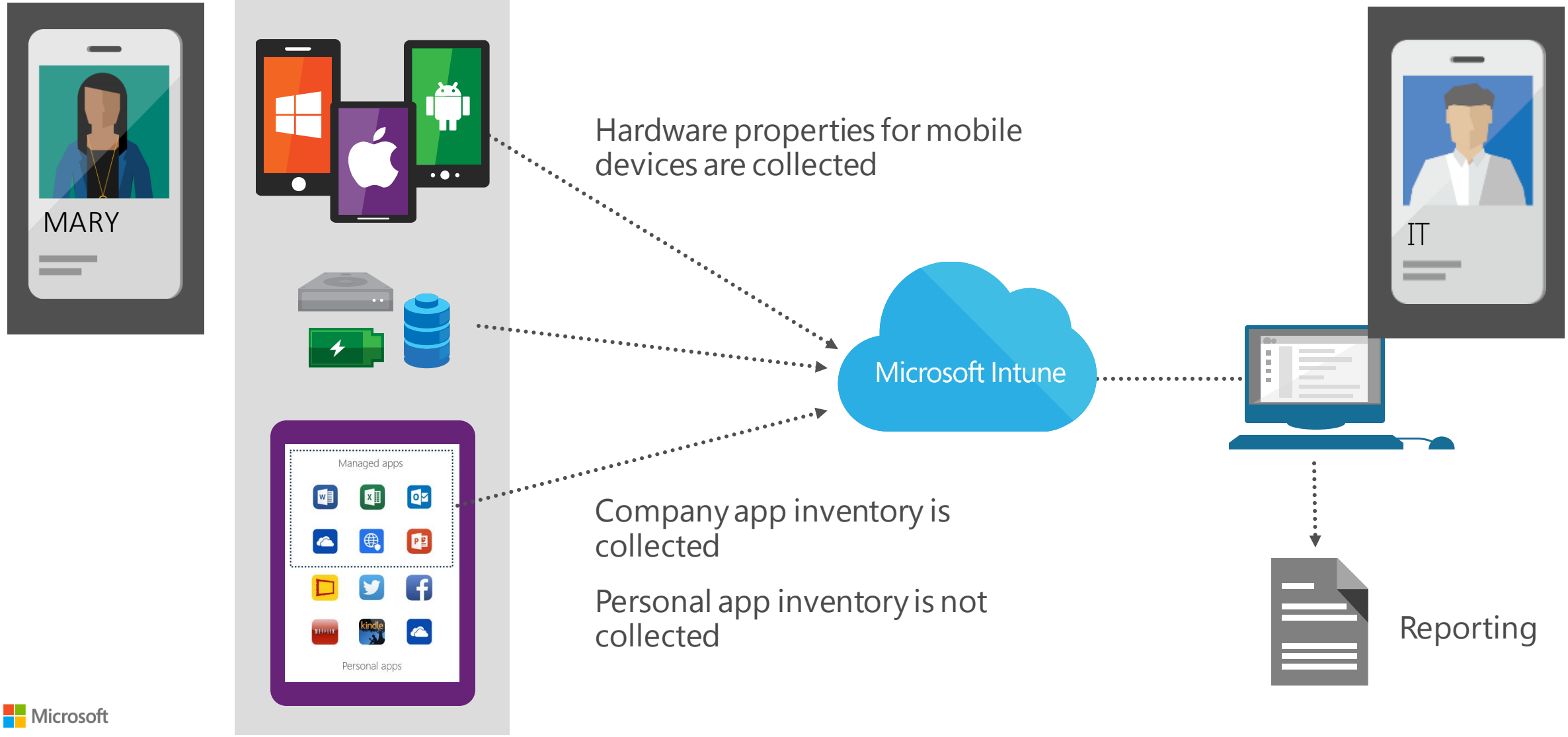
Management of PCs



- Application management
- Software updates
- Inventory and reporting
- Endpoint protection
- Windows firewall
- Remote assistance

Microsoft Intune

Mobile device inventory



Microsoft

Microsoft Intune

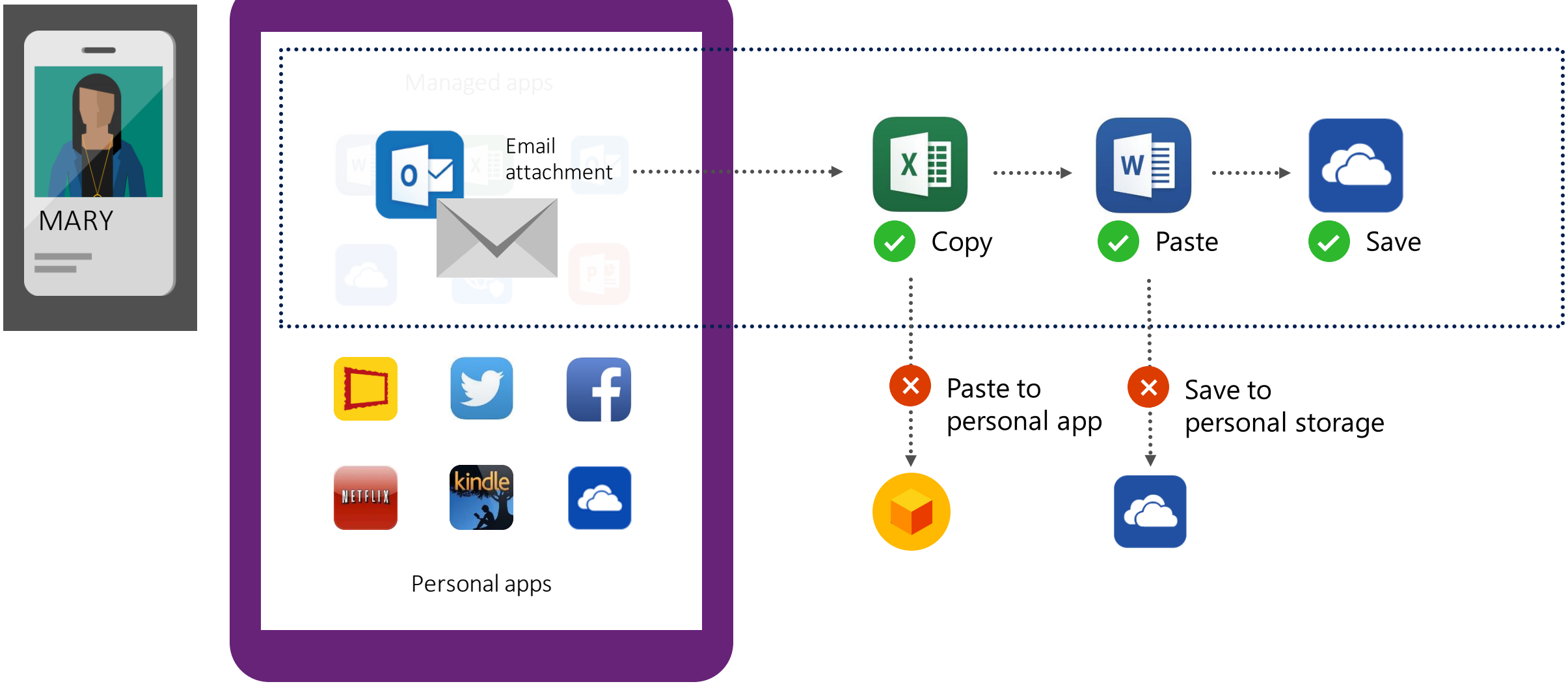
Corporate application management

- Enforce corporate app data access requirements
- Prevent data leakage
- Enforce encryption of app data
- Selective wipe of data at app level

Microsoft

Microsoft Intune

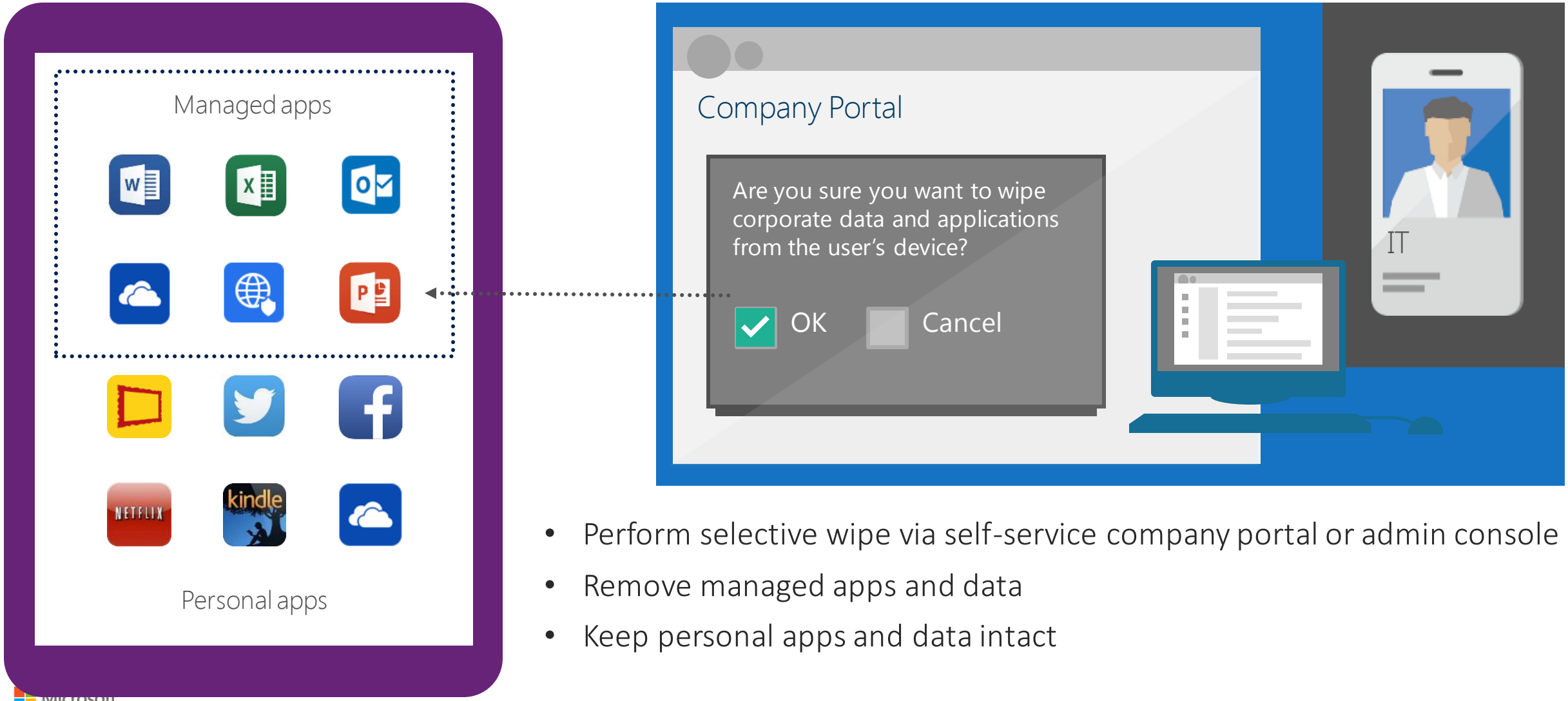
Mobile data protection



Microsoft

Microsoft Intune

Remote selective wipe



- Perform selective wipe via self-service company portal or admin console
- Remove managed apps and data
- Keep personal apps and data intact

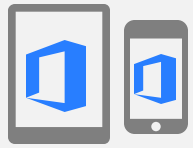
Microsoft Intune

Feature overview and comparison to Office 365

	Mobile Device & Application Management Features	MDM for Office 365	Microsoft 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 Built-in MDM Value	Provides reporting on devices that do not meet IT policy	●	●
	Group-based policies and reporting (ability to use groups for targeted device configuration)	●	●
	Root and jailbreak detection	●	●
	Remove Office 365 app data while leaving personal data and apps intact (selective wipe)	●	●
	Prevent access to corporate email and documents using policy settings	●	●
	Identity management and single sign-on	●	
	Multi-factor authentication	●	
	Rights management data protection	●	
Comprehensive Mobile Device & App Management	Self-service Company Portal for users to enroll their own devices and install corporate apps		●
	App deployment (Windows Phone, iOS, Android)		●
	Deploy certificates, VPN profiles (including app-specific profiles), email profiles, and Wi-Fi profiles		●
	Prevent cut/copy/paste/save as of data from corporate apps to personal apps		●
	Secure content viewing via Managed Browser, PDF Viewer, Imager Viewer, and AV Player apps		●
	Remote device lock via self-service Company Portal and via admin console		●
PC Management	Client PC management (e.g. Windows 8.1, inventory, antimalware, patch, policies, etc.)		●
	PC software management		●

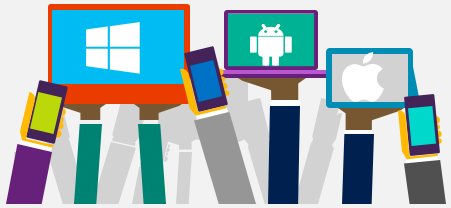
Microsoft Intune

Why mobility management from Microsoft?



It protects Office better

The only solution designed to protect your Microsoft Office email, files, and apps.



It's comprehensive

It protects and manages iOS, Android, Windows devices, Office 365, and LOB apps.

It's simple and easy to use

It's simple to setup, easy to manage and easy for business users.

It's cost-effective

No infrastructure needed, fully cloud-based solution, always up to date. Per-user licensing.

Microsoft Thank you