

#POWERCON2022

Microsoft Intune: gestione dei dispositivi aziendali a 360 gradi

Nicola Ferrini

Microsoft MVP – Cloud and Datacenter Management



/nicolaFerrini.it



@nicolaFerrini



/nicolaFerrini

Agenda

- Market trends
- Microsoft Intune
- Paths to modern management
- Device lifecycle
- Microsoft 365 business value

Technology needs are evolving in the modern workplace

Old world versus new world

Single corporate-owned device



Multiple BYOD devices and IoT devices

Business owned



User and business owned

Corporate network and legacy apps



Cloud managed and SaaS apps

Manual and reactive



Automated and proactive

Corporate network and firewall



Expanding perimeters

Employees



Employees, partners, customers, bots

Mostly onsite employees



Remote and hybrid environment

Top endpoint management challenges



Distributed workers

Remote and hybrid work environments



Endpoint diversity

Multiple devices and app platforms



Employee satisfaction

Easy, fast access to company resources



Cybersecurity

Mitigating risk and vulnerabilities

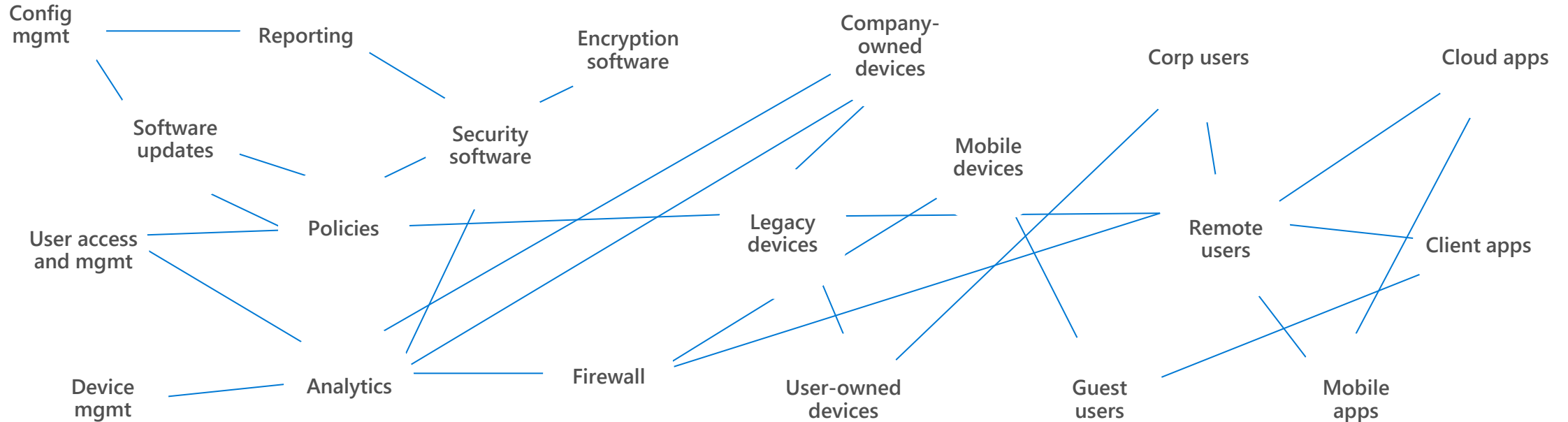


Figure 1: Magic Quadrant for Unified Endpoint Management Tools

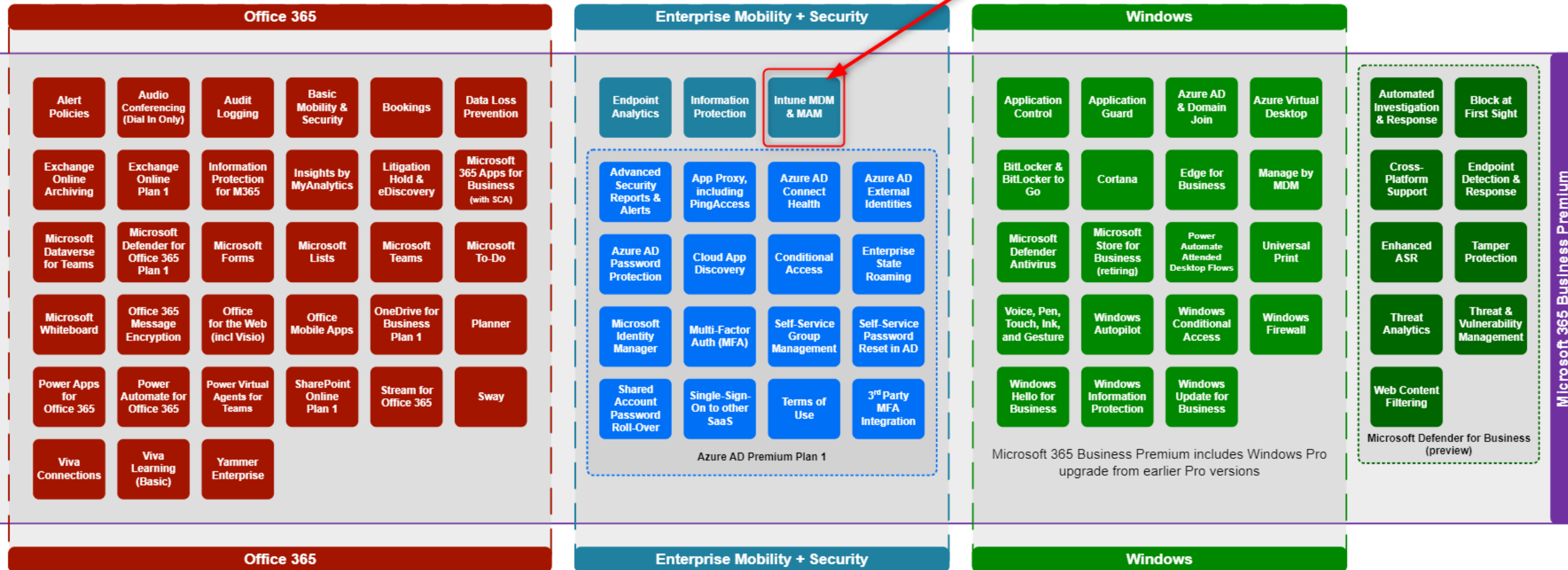


Source: Gartner (August 2021)

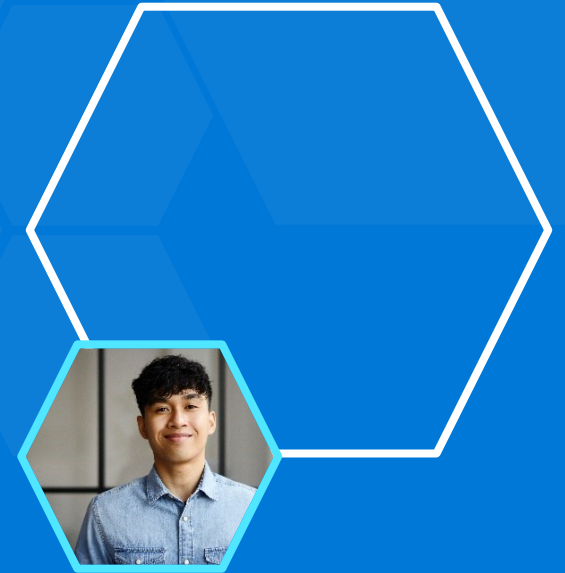
Microsoft 365 Business Premium License

Microsoft 365 Business Premium January 2022

m365maps.com



Microsoft Intune



Microsoft Intune

Microsoft Intune provide the modern management of endpoints with the protection of a Zero Trust strategy.

Protect apps and devices for a resilient workforce

Maximize digital investment with co-management

Get integrated Conditional Access controls

Use simplified management workflows

Secure managed and unmanaged devices and apps



What does Microsoft Intune enable?

Unified management

Apps, device controls, and insights are brought together in one cloud-based endpoint management platform.

Built-in protection

IT is empowered to apply the controls needed for a Zero Trust security model and protect their digital estate without getting in the way of user productivity.

Comprehensive scalability

Intuitive management controls, workflows, and analytics ensure healthy and compliant device and app deployments.



Unified management

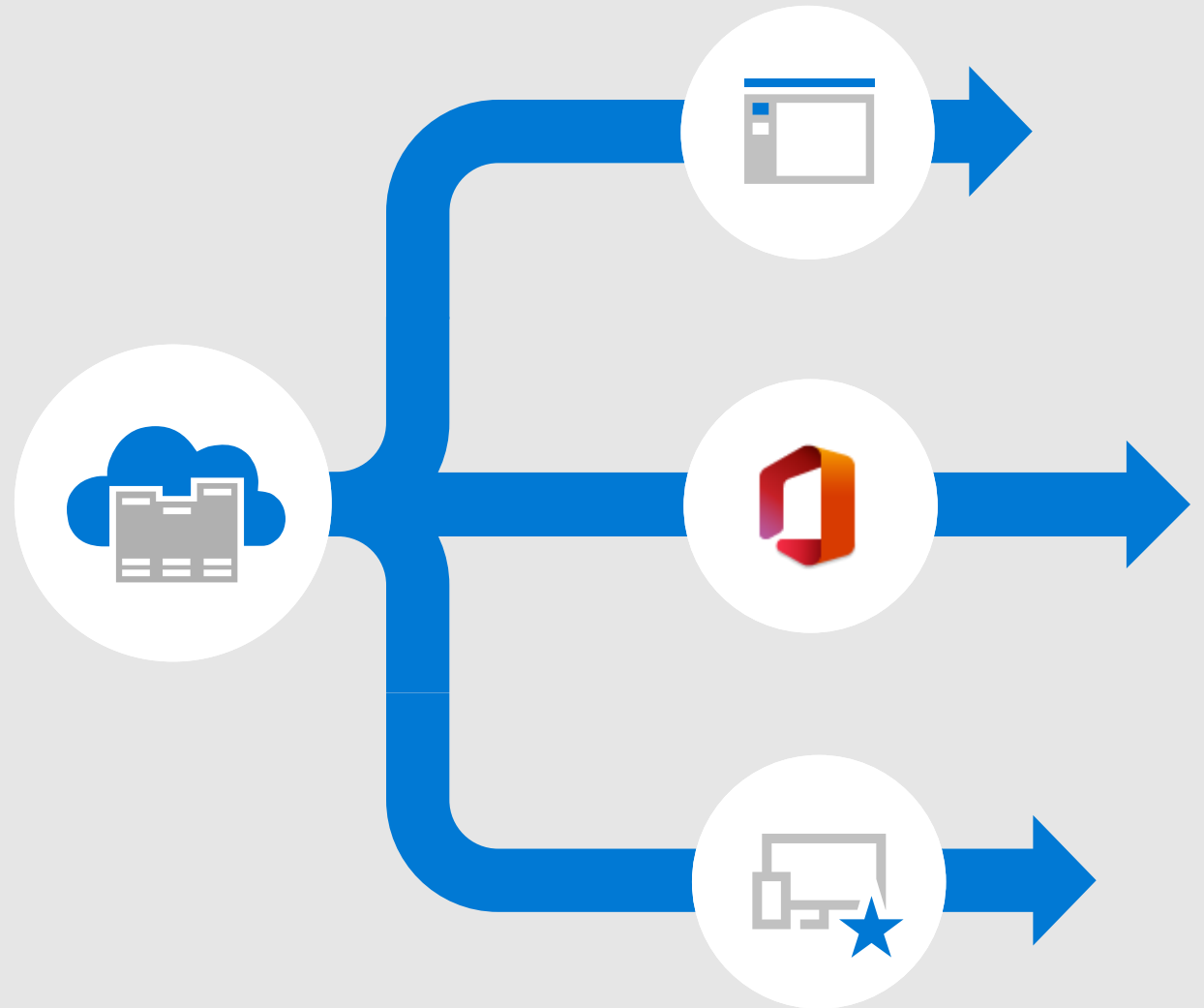
Provide business continuity for remote and hybrid workers

Protection for data on managed and unmanaged devices, whether they're company-owned or personal

Built-in protection with native integration with Microsoft 365 apps and services

Enterprise-grade remote assistance to quickly resolve end-user issues

Touchless provisioning with **Windows Autopilot**



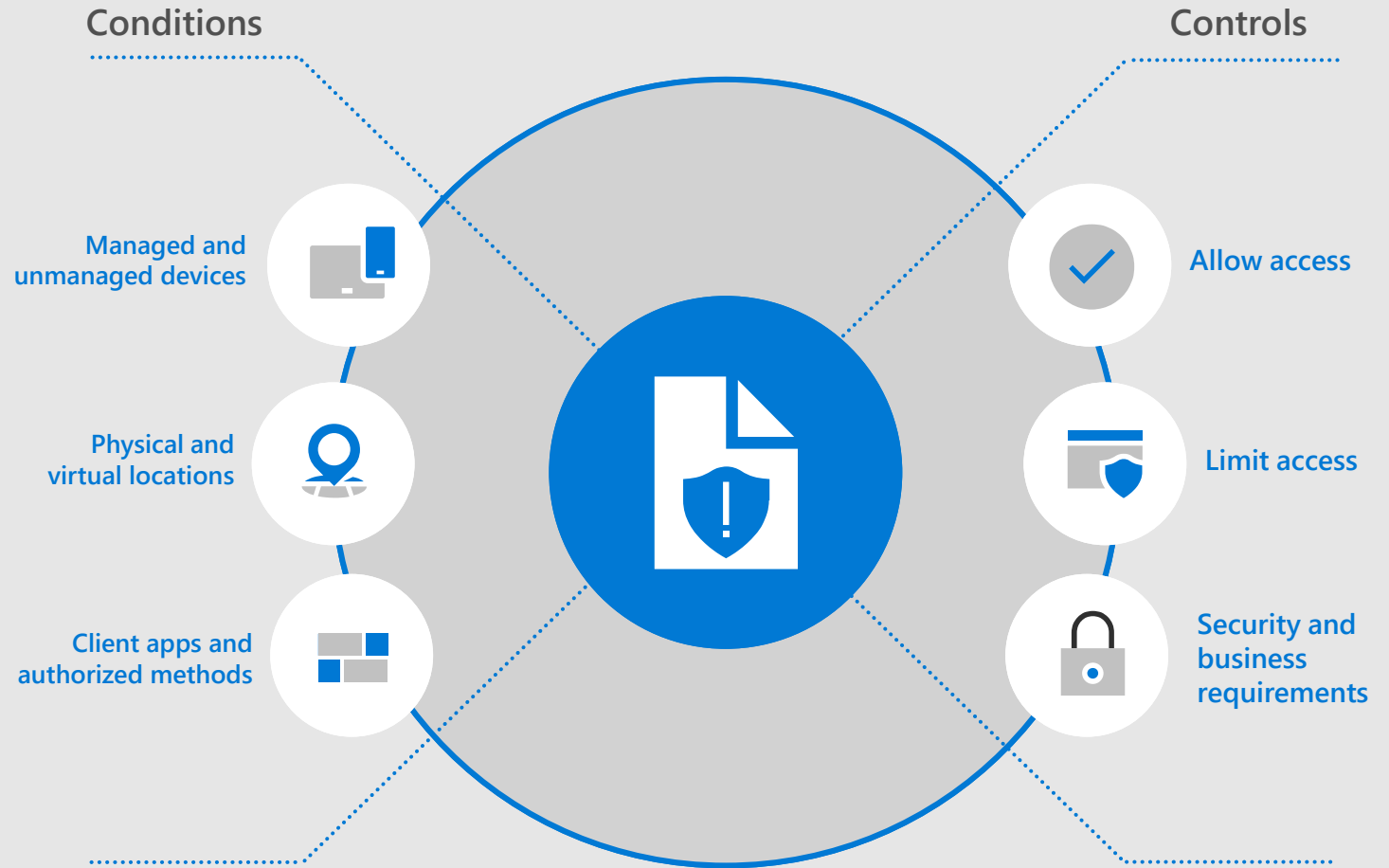
Built-in protection

Protect your company data

Protection for your organization's data, whether it's accessed from managed or unmanaged devices

Conditions can be defined to gate access to your corporate data based on location, device, user state, and application sensitivity

Every device must meet your security and business requirements before accessing your network



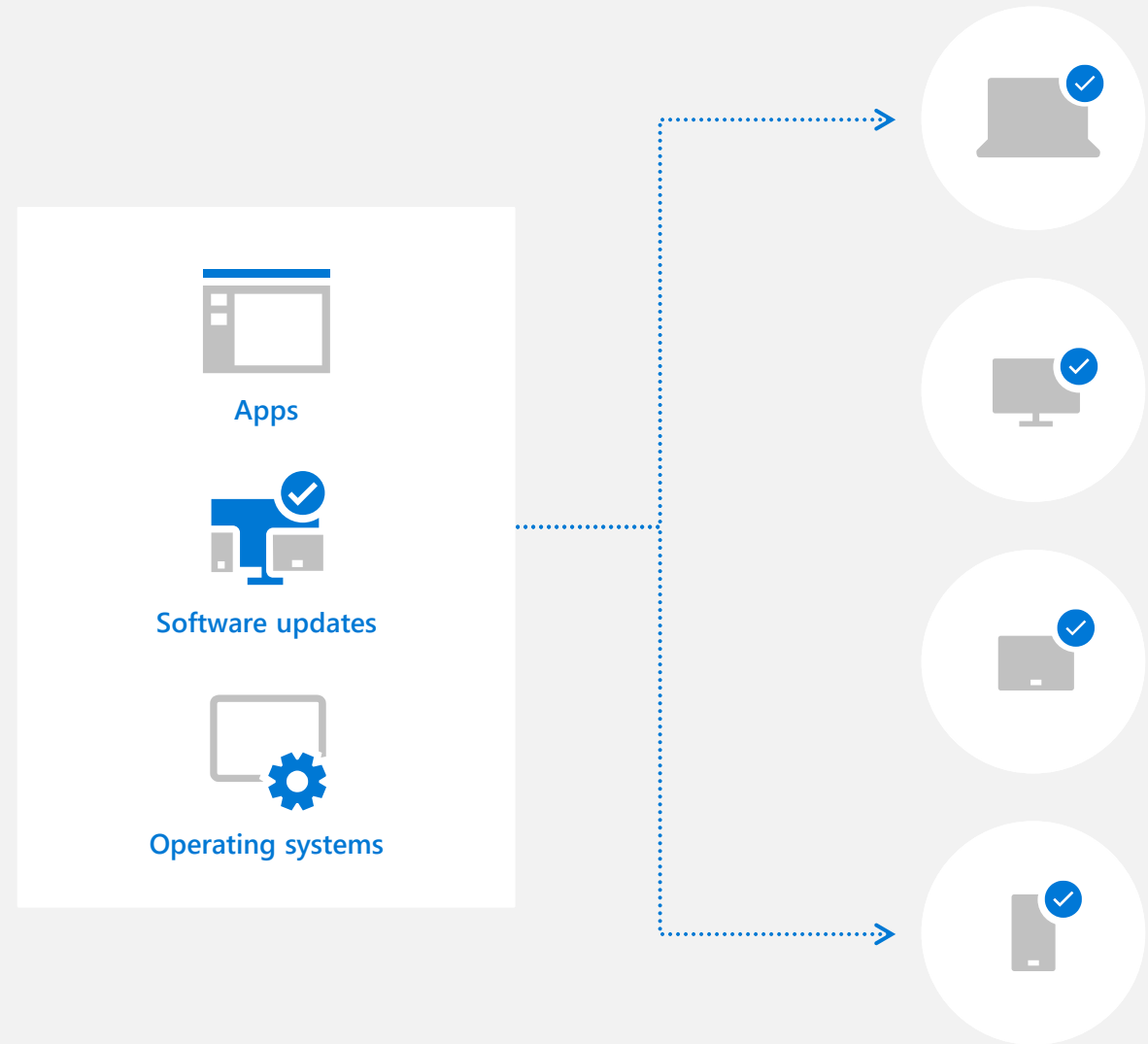
Comprehensive scalability

Simplify and speed deployments

A comprehensive tool for mobile device management (MDM) and mobile application management (MAM) for your apps and devices

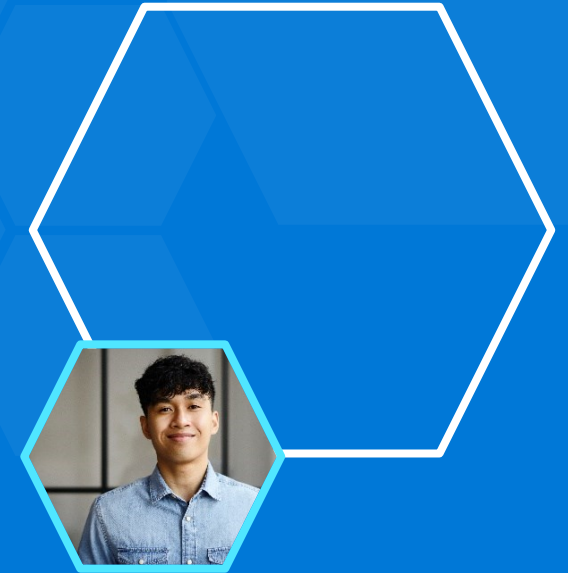
Ability to deploy apps, software updates, and operating systems for desktops, servers, and laptops from on-premises or the cloud

Remote deployment and management of Microsoft Office, including updates and settings





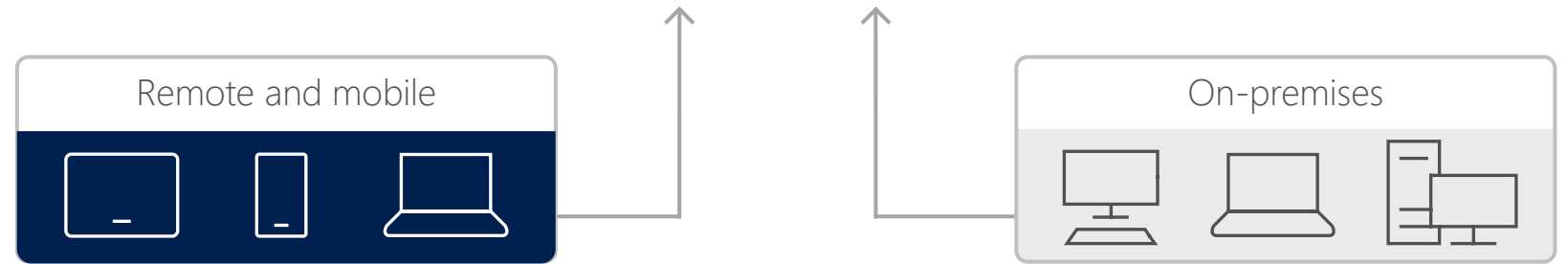
Paths to modern management



Paths to modern management

Microsoft Intune

Limited or no existing management tools



No need to set up and operate your own management infrastructure



Native integration with cloud-powered security controls and risk-based conditional access for apps and data



Flexible support for diverse corporate and BYOD scenarios while increasing productivity and collaboration



Maximize your investment and accelerate time to value with fast rollout of services and devices with end-to-end integration across familiar Microsoft stack

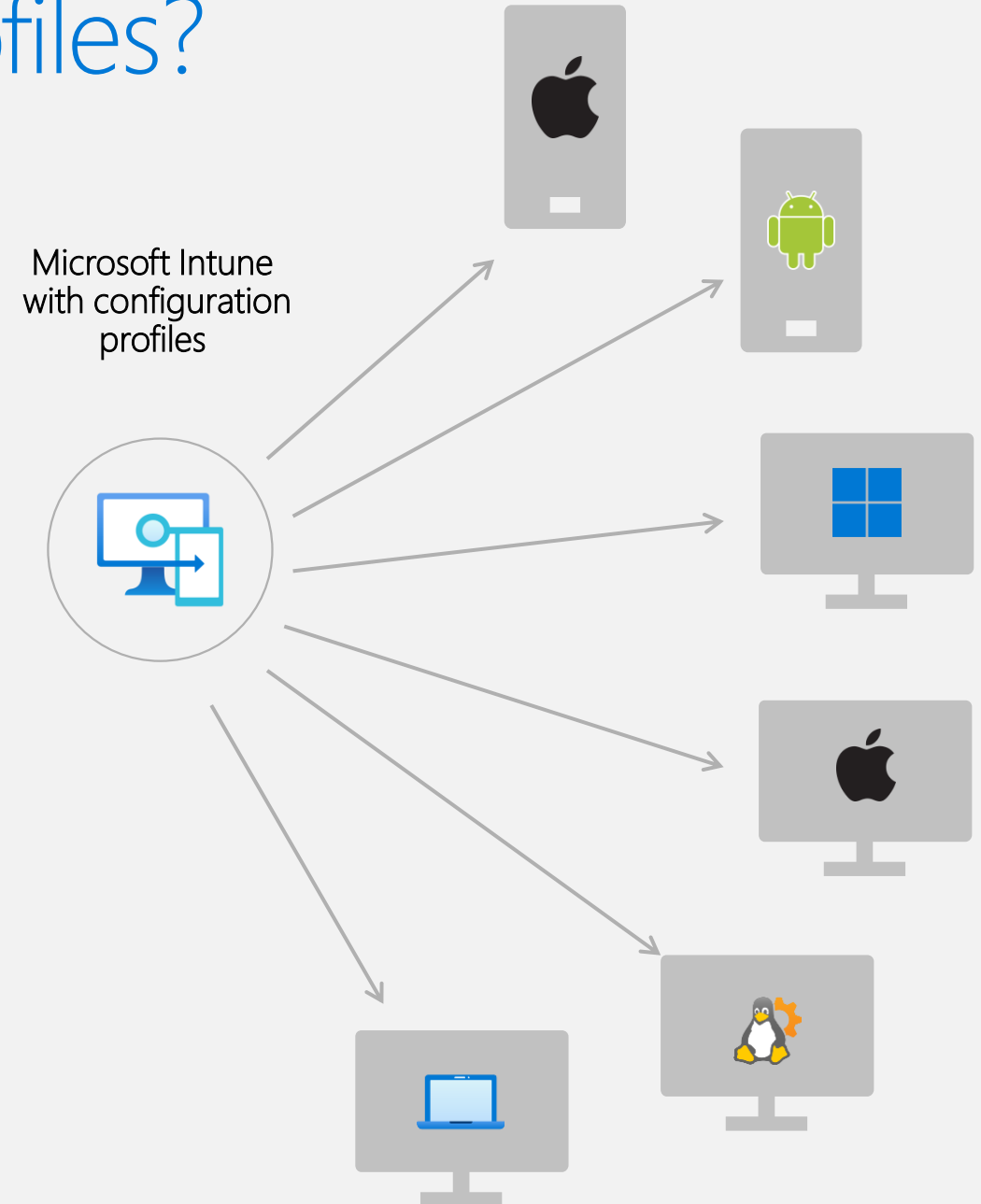
What are configuration profiles?

Microsoft Intune provides configuration profiles which includes settings and features that can be enabled or disabled on different devices within your organization

Configuration profiles can be applied to

- iOS/iPadOS devices
- Android devices
- Windows Client/server devices
- macOS devices
- Linux devices
- ChromeOS devices

[Configuration profiles - ICT Power](#)



What do configuration profiles provide?

Device features

Controls features on the device

Examples: Airprint, notifications and lock screen messages

Device restrictions

Controls security, hardware, data sharing and more settings on the devices

Examples: require a PIN, data encryption, etc

Access configuration

Provide organization's access configuration to the device

Examples: email profiles, VPN profiles, Wi-Fi settings, certificates, etc

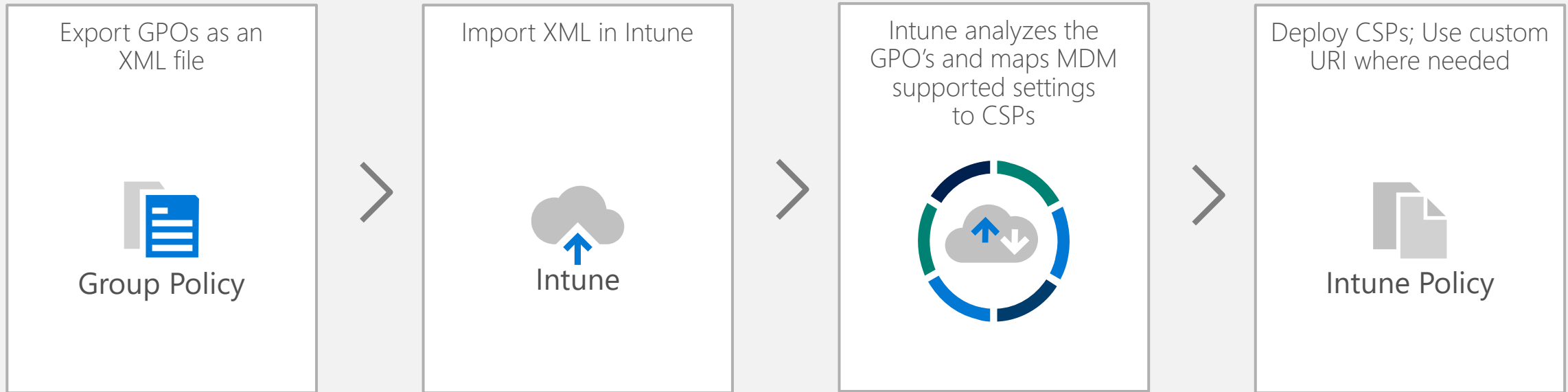
Custom

Set custom configuration or execute custom configuration actions

Examples: set OEM settings, execute PowerShell scripts, etc

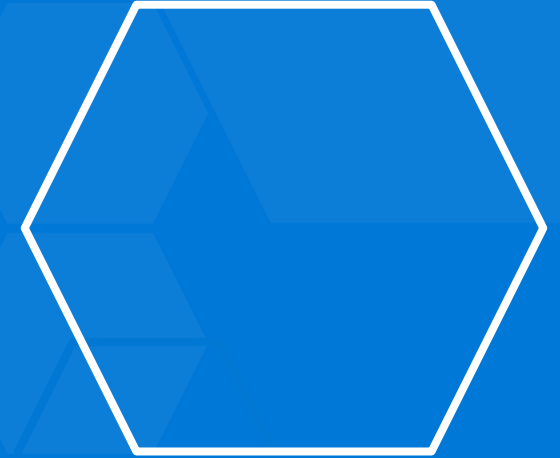
Migrate Windows 10/11 GPOs to Intune

Group Policy analytics compares GPOs to Intune

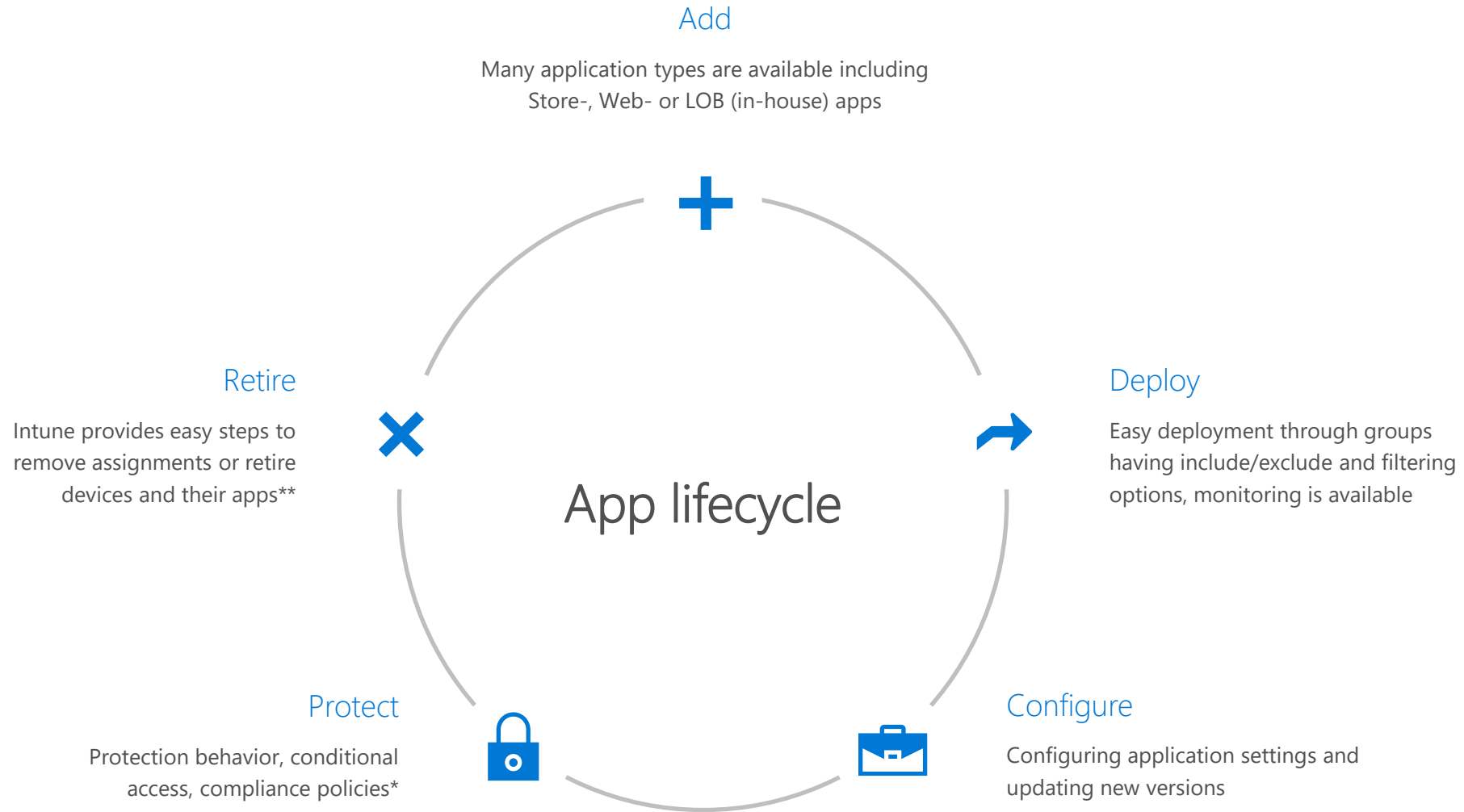


Review the Group Policy Migration Readiness report to see the number of settings in your GPO that are available in a device configuration profile, if they can be in a custom profile, aren't supported, or are deprecated.

Apps deployment



Application lifecycle management in Intune



* Discussed in the Protect session.

** Discussed in the Support and Retire session.

Supported app types

Platform specific app type	General type	App-specific procedure for adding to Intune	Updates
Android line-of-business (LOB) apps	LOB app	Select Line-of-business app as the app type, select the App package file, and then enter an Android installation file with the extension .apk.	You must update the app.
iOS/iPadOS LOB apps	LOB app	Select Line-of-business app as the app type, select the App package file, and then enter an iOS/iPadOS installation file with the extension .ipa.	You must update the app.
Windows LOB apps	LOB app	Select Line-of-business app as the app type, select the App package file, and then enter a Windows installation file with the extension .msi, .appx, .appxbundle, .msix, and .msixbundle.	You must update the app.
Built-in iOS/iPadOS app	Built-in app	Select Built-In app as the app type, and then select the built-in app in the list of provided apps.	Automatic
Built-in Android app	Built-in app	Select Built-In app as the app type, and then select the built-in app in the list of provided apps.	Automatic
Web apps	Web app	Select Web link as the app type, and then enter a valid URL pointing to the web app..	Automatic
Android Enterprise system apps	Store app	Select Android Enterprise system app as the app type, and then enter the app name, publisher, and package file.	Automatic
Windows app (Win32)	LOB app	Select Windows app (Win32) as the app type, select the App package file, and then select an installation file with the extension .intunewin.	You must update the app.
macOS LOB apps	LOB app	Select Line-of-business as the app type, select the App package file, and then select an installation file with the extension .intunemac.	You must update the app.

Store app

Android store app

iOS store app

Microsoft Store app (new)

Microsoft Store app (legacy)

Managed Google Play app

Microsoft 365 Apps

Windows 10 and later

macOS

Microsoft Edge, version 77 and later

Windows 10 and later

macOS

Microsoft Defender for Endpoint

macOS

Web Application

iOS/iPadOS web clip

Windows web link

Other

Web link

Built-In app

Line-of-business app

Windows app (Win32)

Microsoft Intune app protection policies

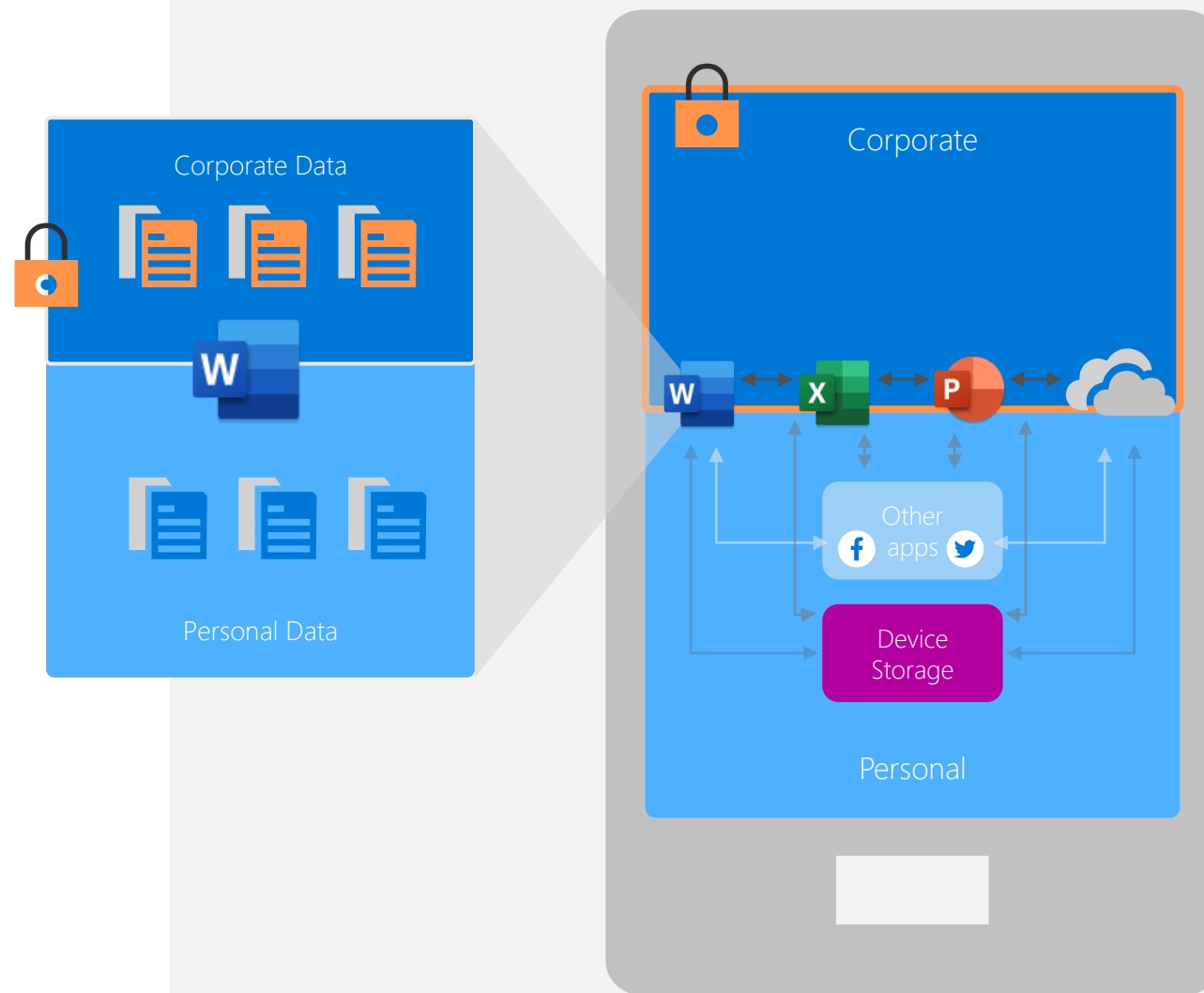
Microsoft Intune provides app protection policies (APP), which are app-level rules that can manage and protect your organization's corporate data

App protection policies can be applied to

iOS/iPadOS devices (iPhones, iPads, iPods)*

Android devices

Windows devices



What do app protection policies provide?



Multi-identity awareness

Targets protection ONLY to corporate account

Personal and unmanaged accounts aren't affected



Data protection

Encrypts corporate data

Controls data transfer mechanisms between managed and unmanaged apps

Controls transfer of web content

Selective wipe of corporate data – whether it be admin, user, or offline initiated



Access requirements

Controls access to corporate data via PIN, biometrics, or credentials

Provides inactivity timers



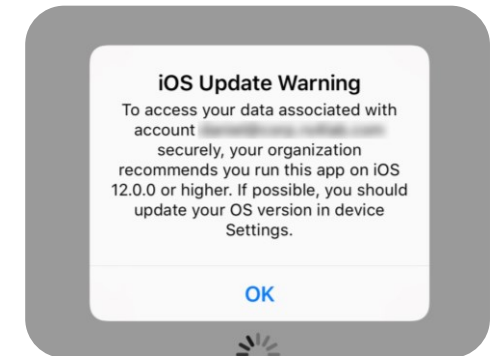
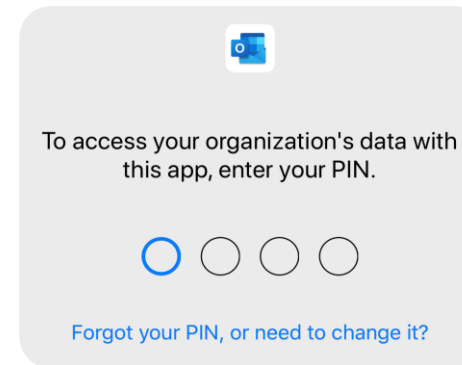
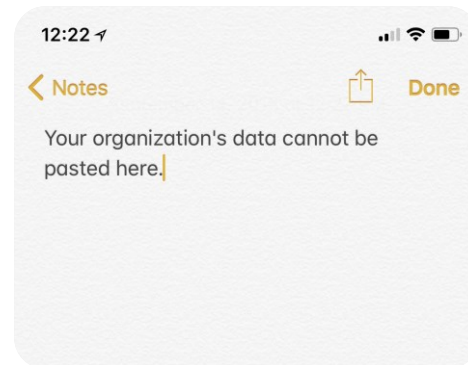
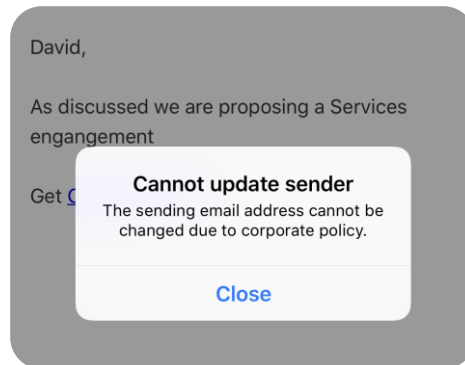
Conditional launch

Validates device health: Jailbreak/Rootkit, mobile threat defense

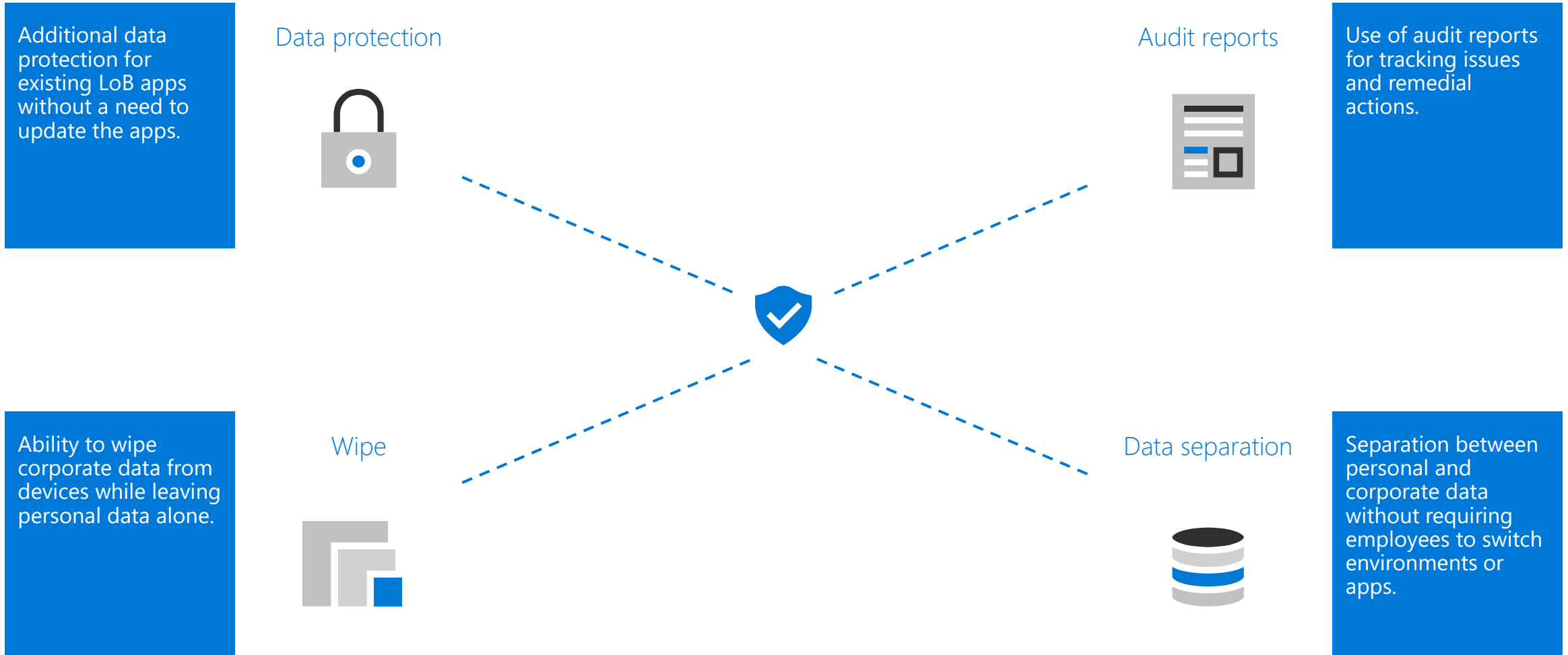
Validates OS variables like OS version, Android patch version

Validates app variables like app version or SDK version

Validates device model or manufacturer



What do app protection policies provide?



Endpoint security policies



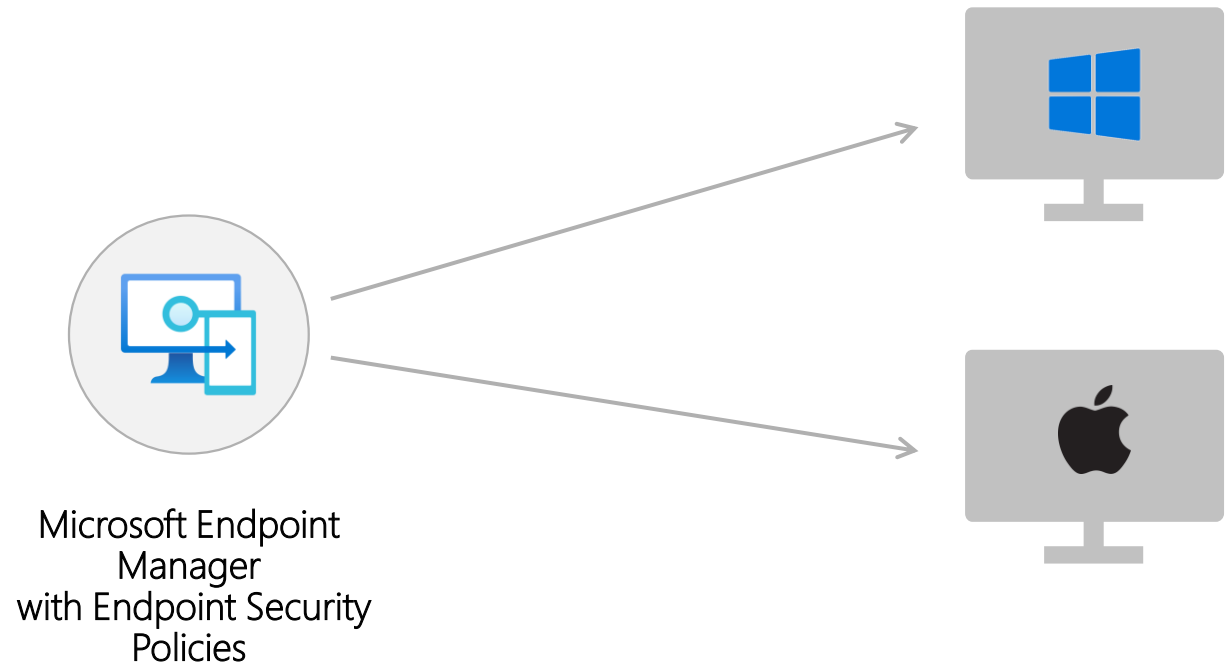
Microsoft Intune endpoint security policies

Microsoft Intune provides endpoint security policies, which are tightly focused device-level security settings that determine the configuration of:

Antivirus, disk encryption, firewalls

Several areas made available through integration with Microsoft Defender for Endpoint

Endpoint security policies can configure device security without the overhead of navigating the larger range of settings from device configuration profiles and security baselines



What do endpoint security policies provide?

Firewall settings



Account protection settings



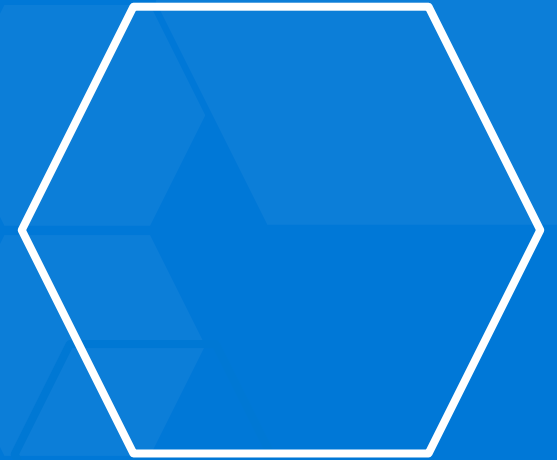
Microsoft Defender for Endpoint settings



Disk encryption settings



OS updates



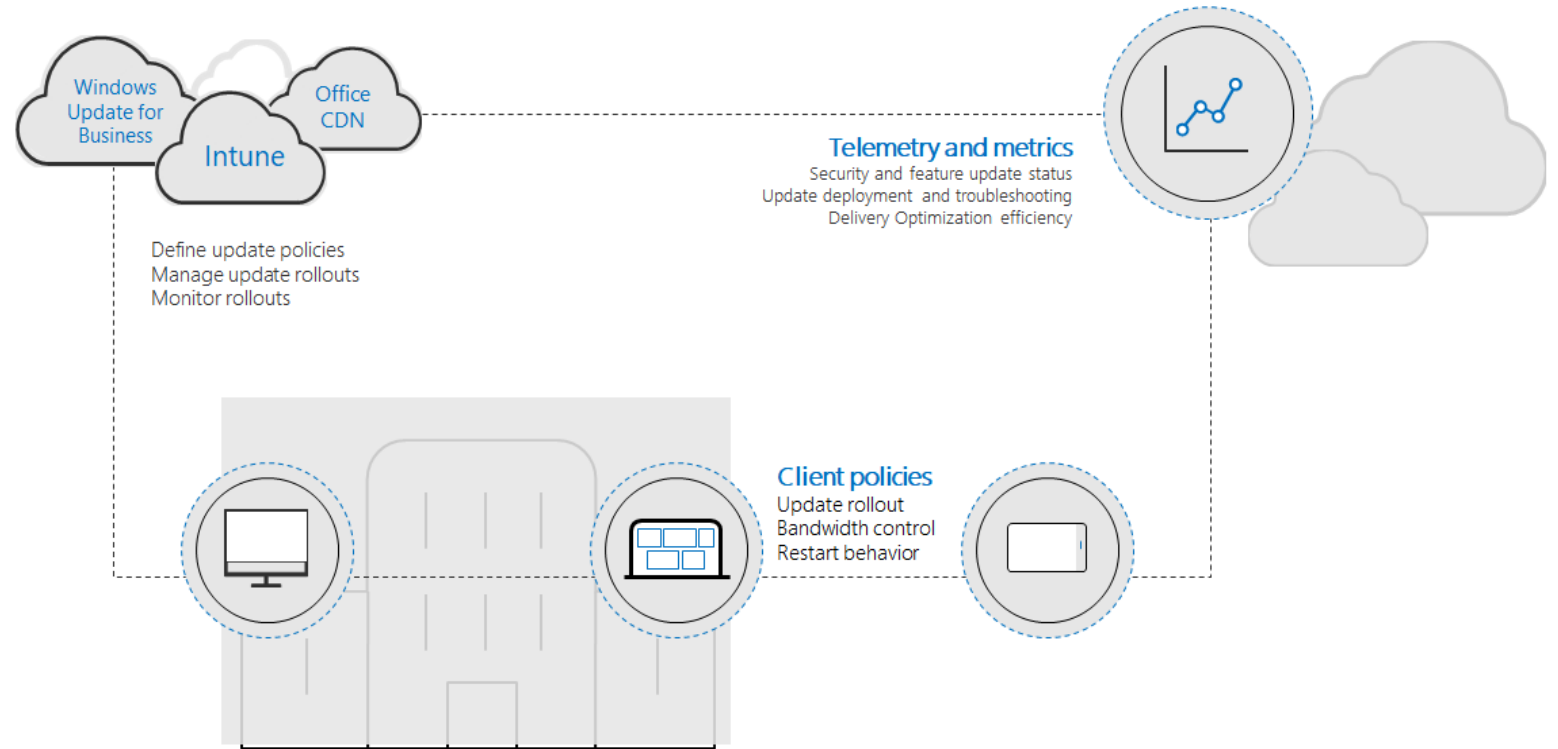
Keeping Windows up-to-date with Microsoft Intune and Windows Update for Business

Microsoft Endpoint Manager

Provides OS update policies for Windows to enrolled devices

Windows Update for Business

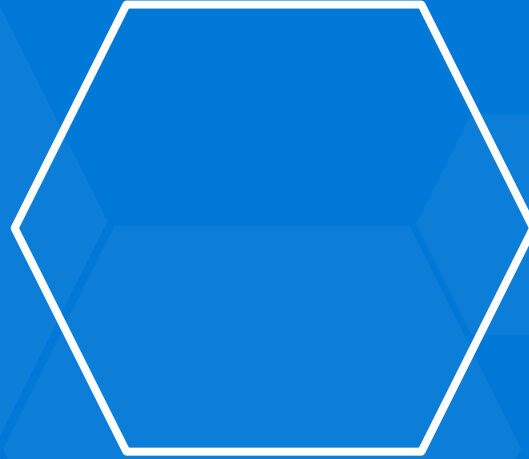
Provides actual OS update to devices



Managing updates from the cloud

Reduce on-premises infrastructure and simplify management

Device lifecycle



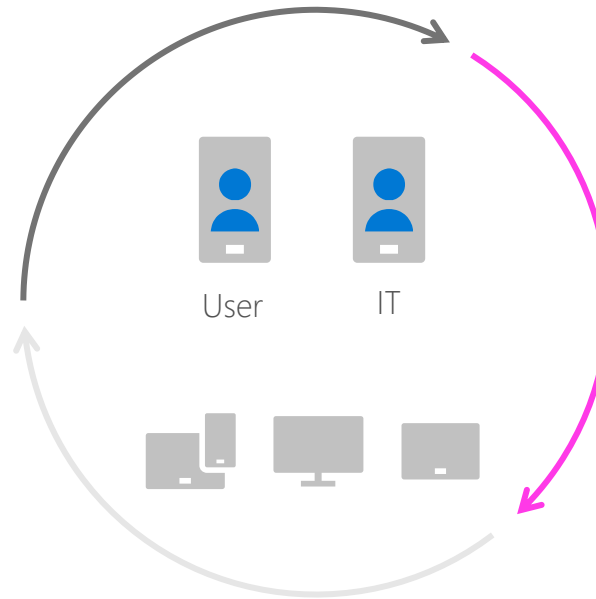
Manage the entire device lifecycle with Microsoft Intune

Enroll

- Provide specific enrollment methods for iOS/iPadOS, Android, Windows, and macOS
- Provide a self-service company portal for users to enroll BYOD devices
- Deliver custom terms and conditions at enrollment
- Zero-touch provisioning with automated enrollment options for corporate devices

Support and retire

- Revoke access to corporate resources
- Perform selective wipe
- Audit lost and stolen devices
- Retire device
- Provide remote assistance



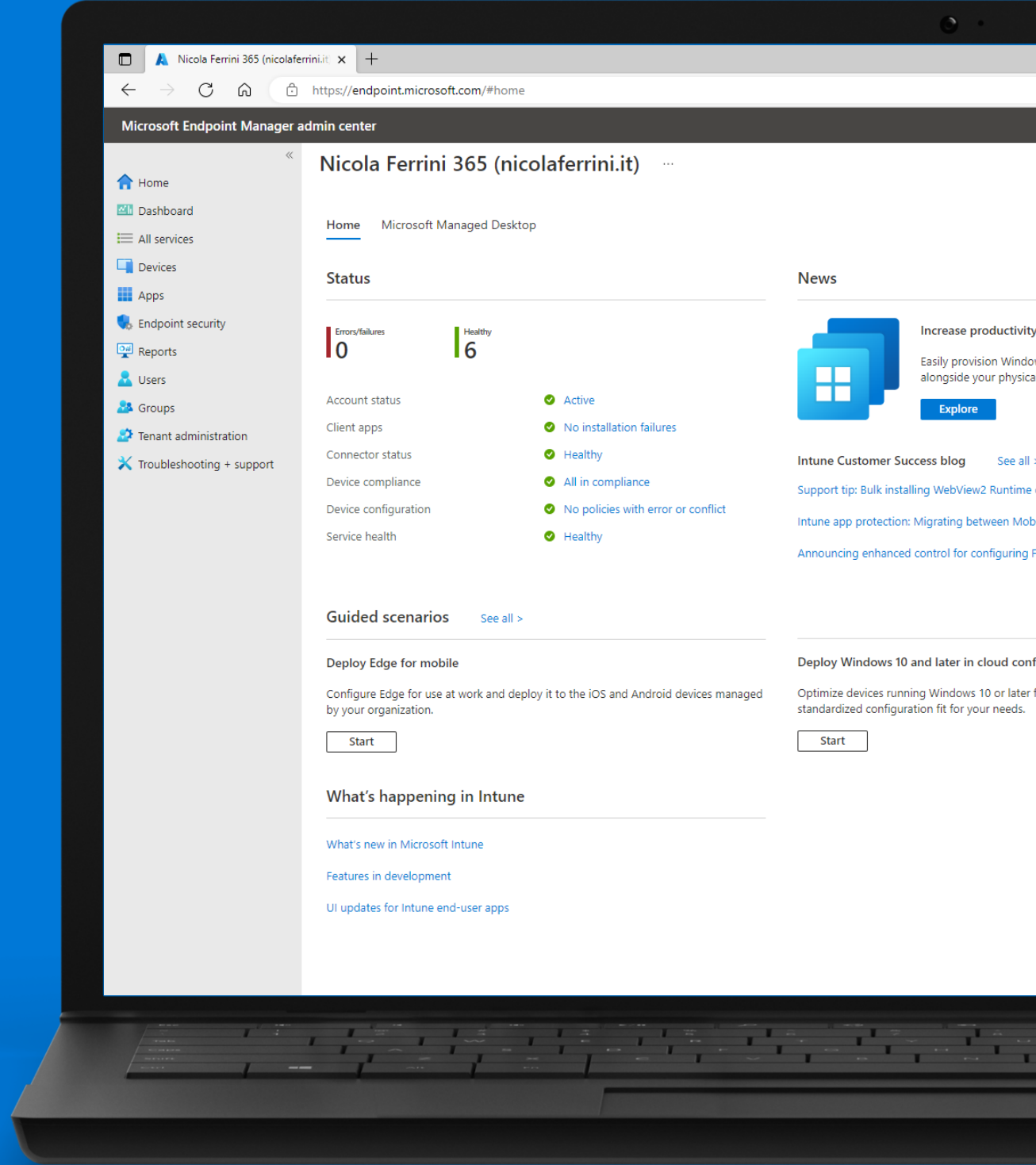
Configure

- Deploy certificates, email, VPN, and Wi-Fi profiles
- Deploy device security policy settings
- Install mandatory apps
- Deploy device restriction policies
- Deploy device feature settings

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

DEMO



Grazie



/nicolaferri.it



@nicolaferri



/nicolaferri