Unified Device Management with Windows Intune

Andras Khan
Microsoft Western Europe HQ

Microsoft

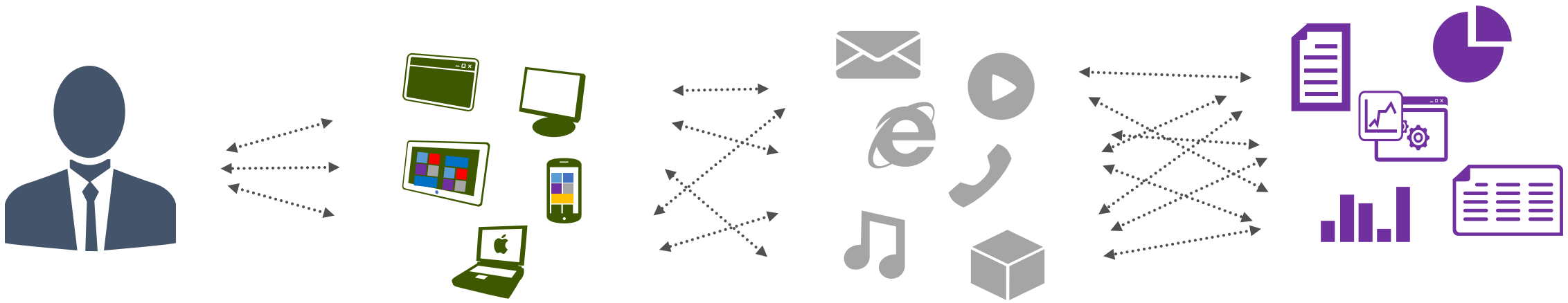
Windows Intune

Microsoft System Center 2012 R2
Configuration Manager

Agenda

- What are the challenges we are seeing cross vertical
- Unified Device Management Strategy
- How Unified Device Management can help address those challenges
- So what are the benefits of UDM
- Key Takeaways
- Q&A

Today’s challenges



Users

Users expect to be able to work in any location and have access to all their work resources.

Devices

The explosion of devices has eradicated the standards based approach to corporate IT.

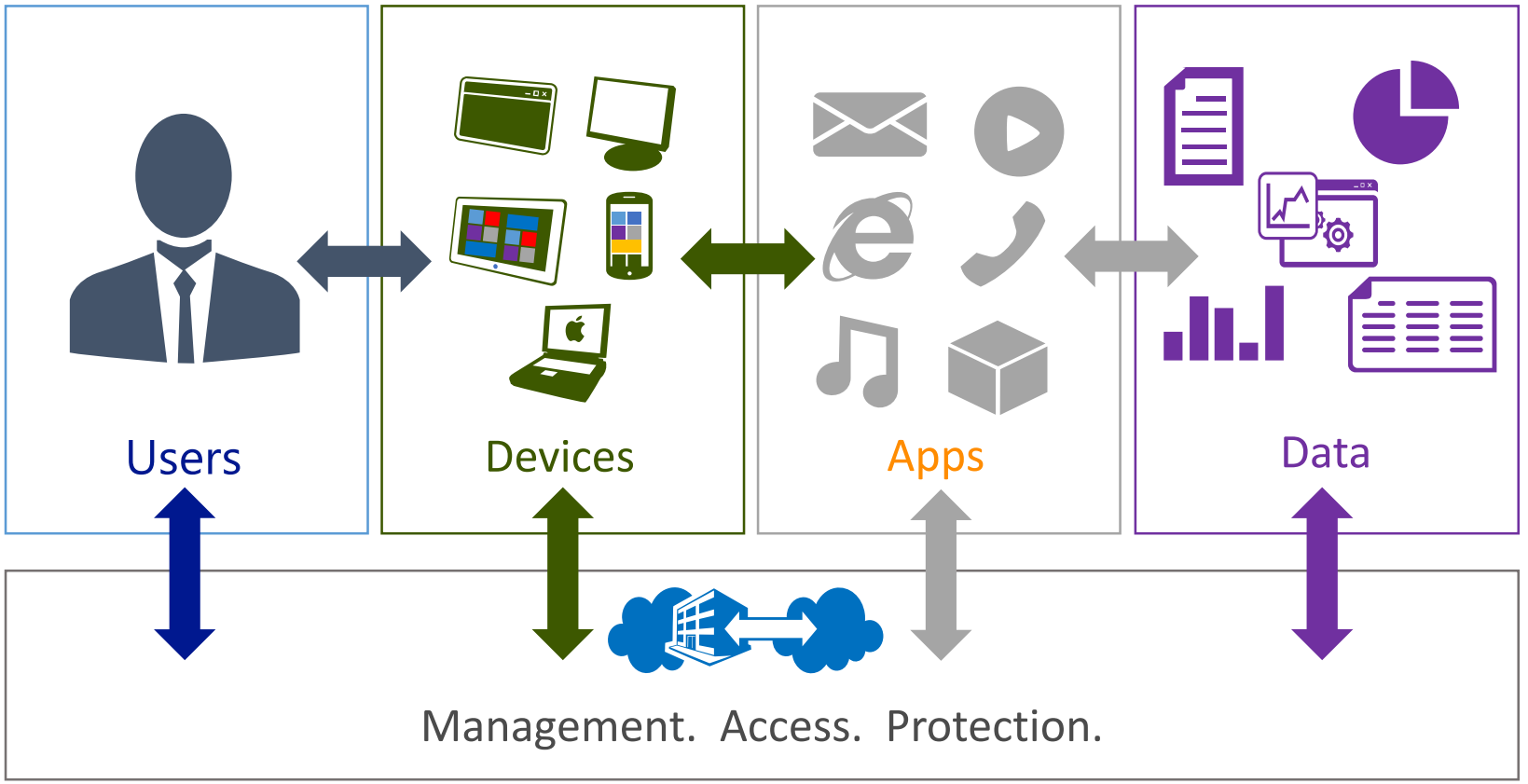
Apps

Deploying and managing applications across platforms is difficult.

Data

Enabling users to be productive while maintaining compliance and reducing risk.

People-centric IT



Empower users

Allow people to work on the device of their choice and provide consistent access to corporate resources.

Unify your environment

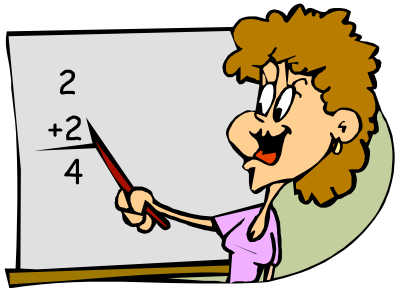
Deliver a unified application and device management on-premise and in the cloud.

Protect your data

Help protect corporate information and manage risk.

Windows Intune + SCCM 2012 R2

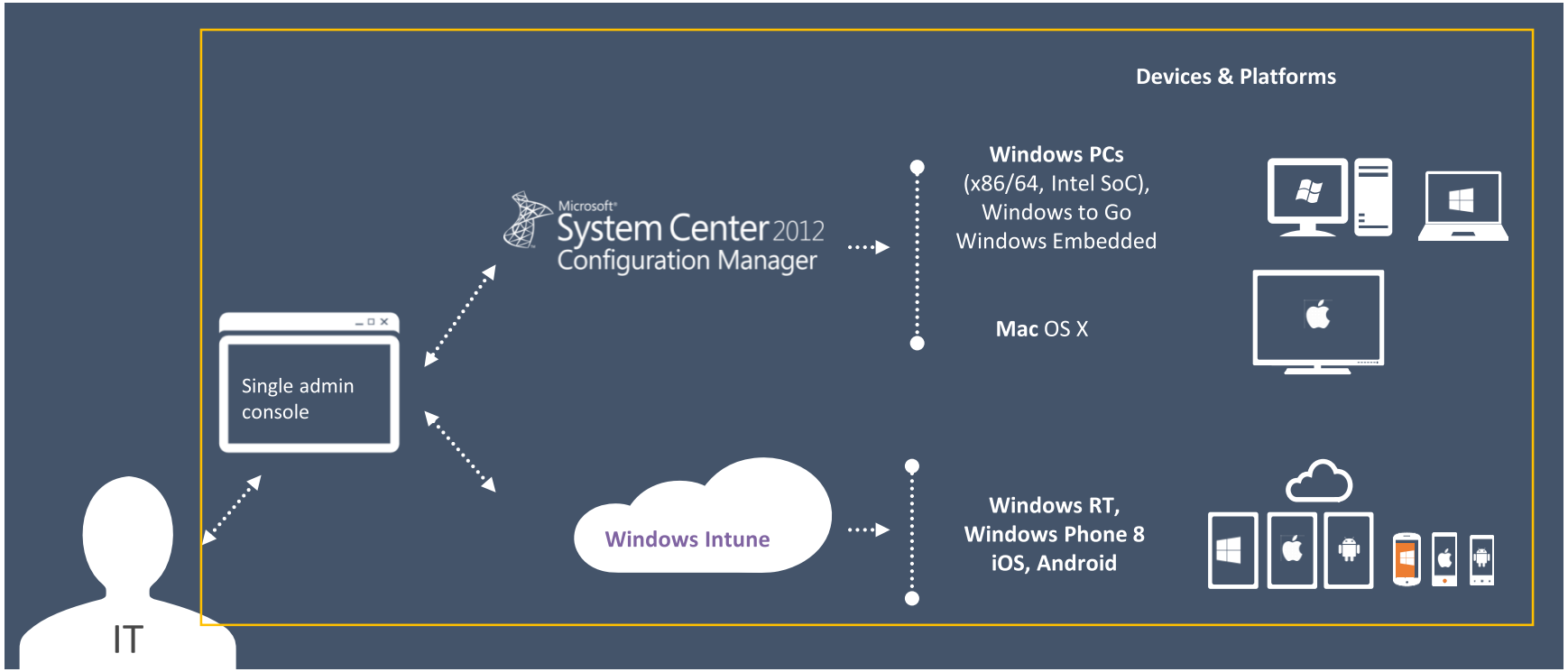
Value proposition: “Realize the benefits of Unified Device Management”



- Customers are having silo solutions for device management
  - Silo Solution for on premise domain joined managed devices
  - Silo Solution for mobile device management
  - Silo Solution for non domain joined PCs
- Windows Intune address all of these concerns!
  - On premise domain joined managed devices→ Can be managed by either SCCM or Windows Intune
  - Mobile Device Management → Windows Intune can manage WP8, iOS, Android and Win RT via native management
  - Non domain joined PCs→ Windows Intune can manage all non domain joined PCs

Simplifying Management Across Platforms

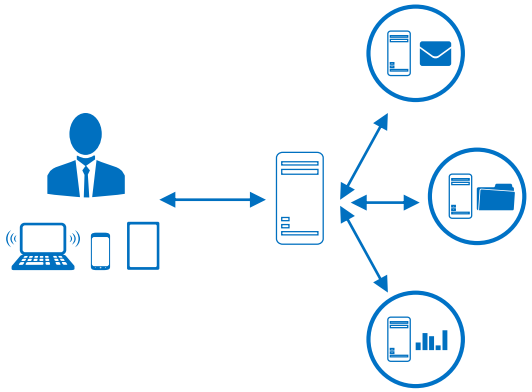
Extended functionality through Unified Solution – Single pane of glass



Strategic Direction

One unified device management solution that **combines on premise and cloud capabilities** into one solution – creating a **cost efficient, secure offering** that enables customers to choose the right delivery mechanism for them.

Unified Device Management

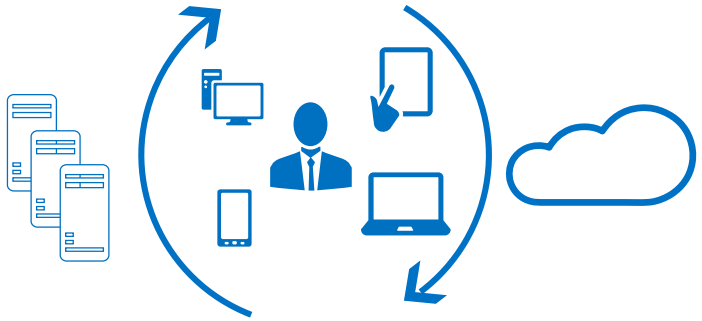


Empower users

Access to company resources consistently across devices

Simplified registration and enrollment of devices

Synchronized corporate data



Unify your environment

On-premises and cloud-based management of devices within a single console.

Simplified, user-centric application management across devices

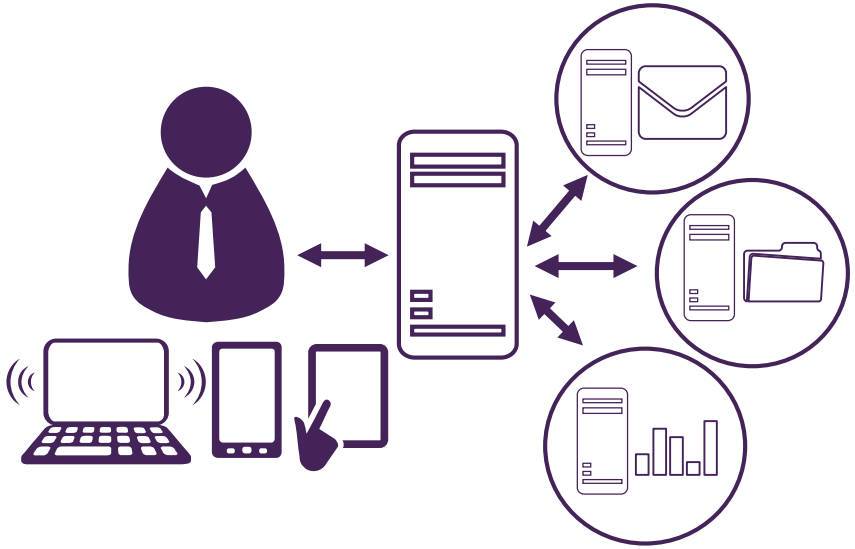
Comprehensive settings management across platforms, including certificates, VPNs, and wireless network profiles

Protect your data

Protect corporate information by selectively wiping apps and data from retired/lost devices

A common identity for accessing resources on-premises and in the cloud

Empower users



Challenges

Users want to **use the device of their choice** and have access to both their personal and work-related applications, data, and resources.

Users want an easy way to be able to **access their corporate applications** from anywhere.

IT departments want to empower users to work this way, but they also need to **control access to sensitive information** and remain in compliance with regulatory policies.

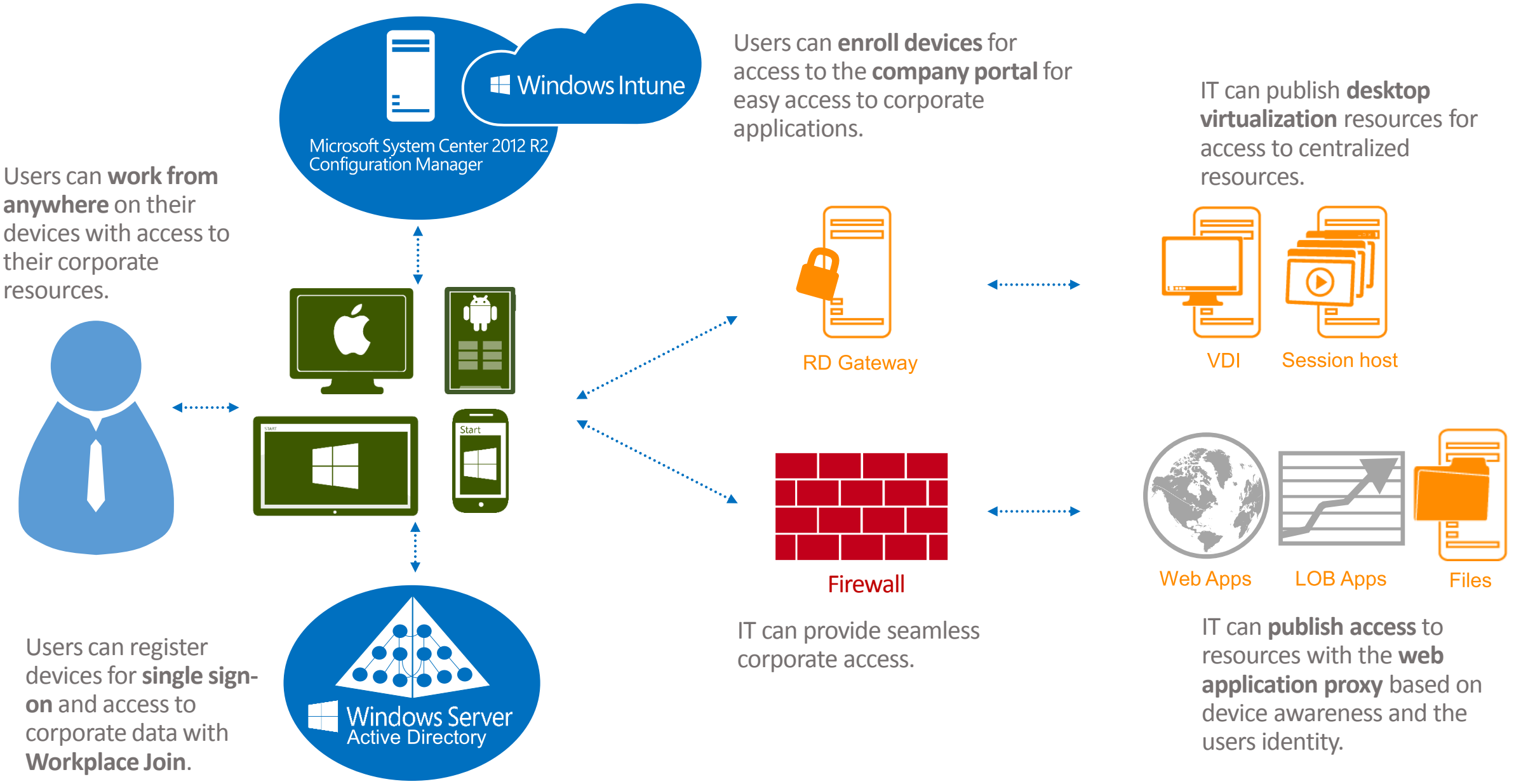
Solutions

Users can **register their devices,** which makes them known to IT, who can then use device authentication as part of providing **access to corporate resources**.

Users can **enroll their devices,** which provides them with the company portal for **consistent access to applications** and data, and to manage their devices.

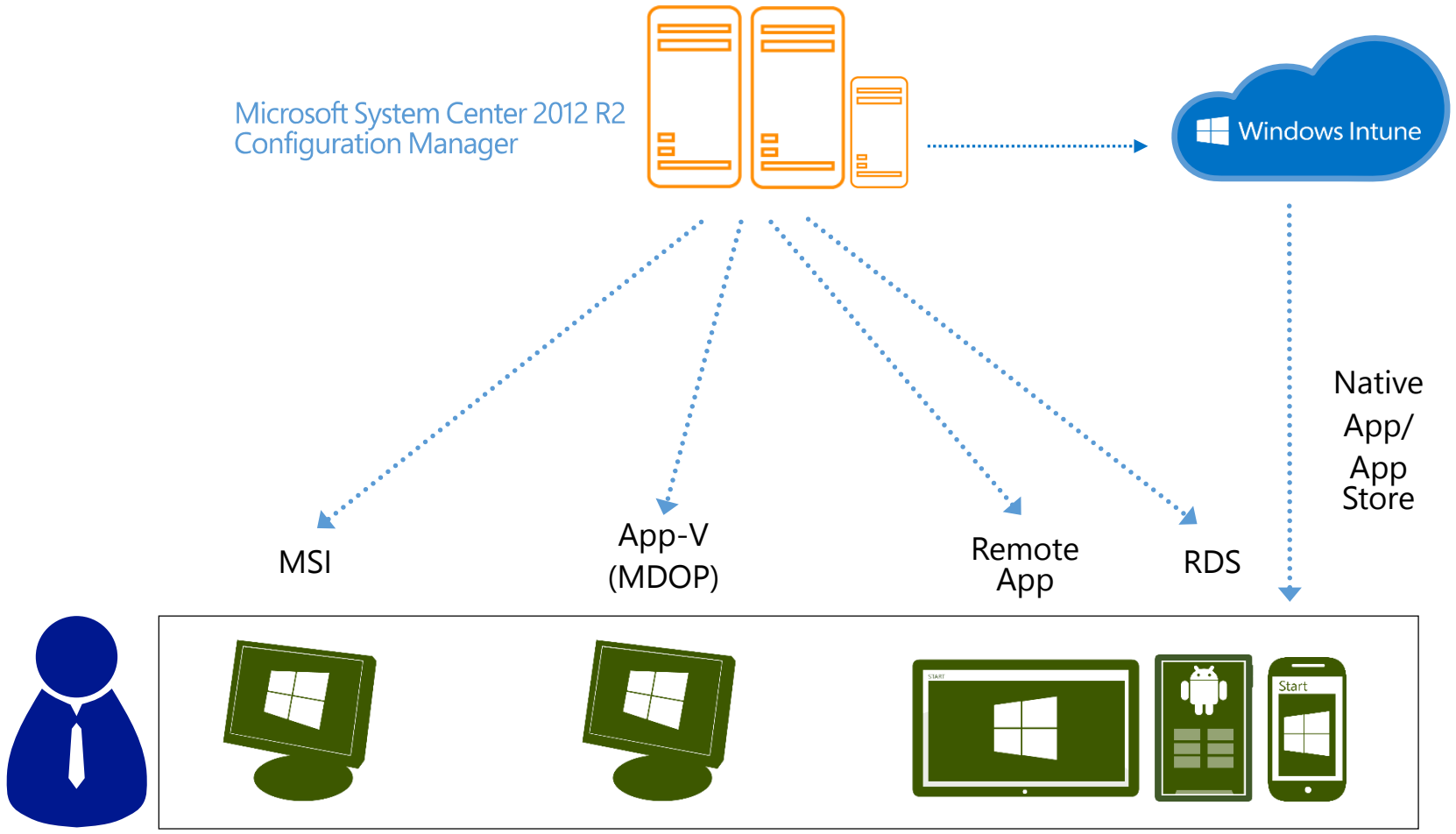
IT can **publish access to corporate resources** with conditional access based on the user's identity, the device they are using, and their location.

Enabling IT to empower users



People-centric Application Delivery

Accessing apps the right way, on the right device



Target applications based on user role the best way for each device

- Windows/Windows RT
- Windows Phone
- iOS
- Android
- OS X

Evaluate device capabilities for optimal application delivery

- Local installation
- Microsoft Application Virtualization
- Desktop Virtualization (VDI)
- Web applications

Unify your environment

Challenges

MDM products are typically delivered as point solutions, which **do not integrate** with the main PC management solution already in use.

Managing multiple identities and keeping the information in sync across environments is a **drain on IT** resources.

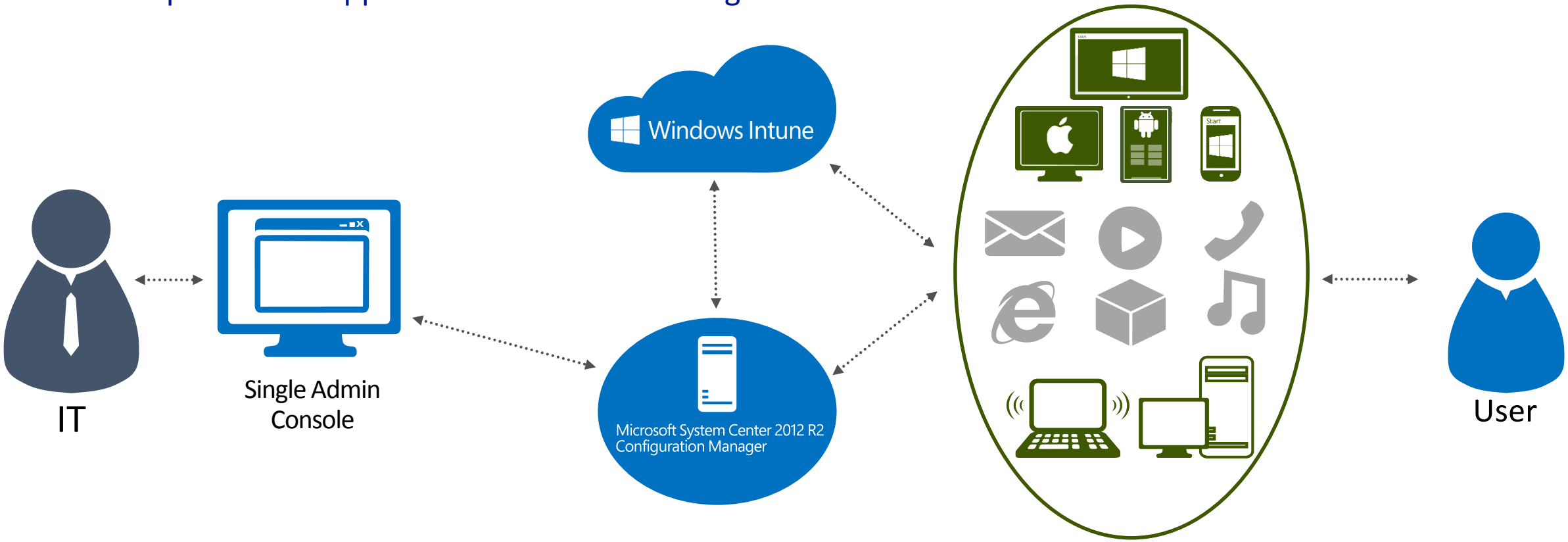
Solutions

IT has a single “pane of glass” **to view and manage all managed devices**, whether on-premises or cloud-based, PCs or mobile devices.

Users and IT can leverage their common identity for access to **external resources through federation**.

Unify your environment

Deliver comprehensive application and device management



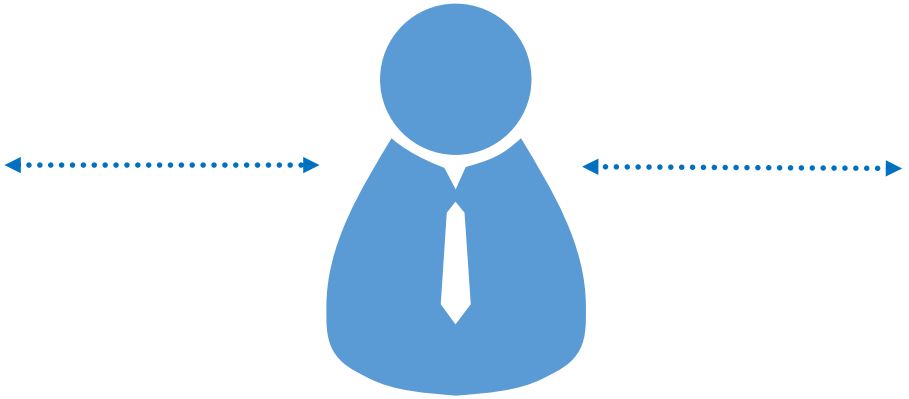
Unified infrastructure enables IT to manage devices “where they live”

Comprehensive settings management across platforms, including certificates, VPNs, and wireless network profiles

IT can manage the device and application lifecycle

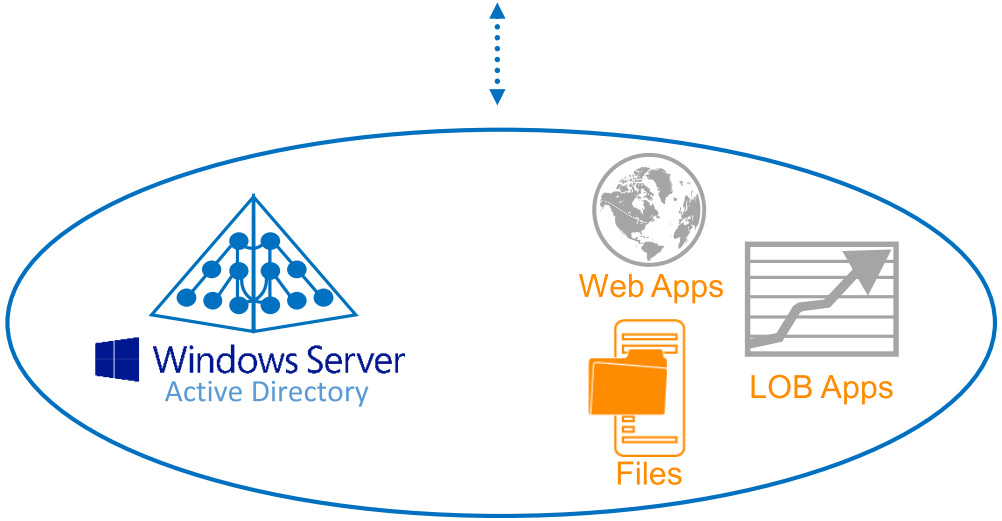
Providing users with a common identity

IT can use **Active Directory Federation Services** to connect with Windows Azure for a consistent cloud-based identity.



Users are more productive by having a **single sign-on** to all their resources.

Users get access through accounts in **Windows Azure Active Directory** to Windows Azure, **Office 365,** and **third-party applications**.



IT can provide users with a common identity across on-premises or cloud-based services, leveraging **Windows Server Active Directory** and **Windows Azure Active Directory**.

Developers can build applications that leverage the common identity model .

Protect your data

Challenges

As users **bring their own devices** in to use for work, they will also want to **access sensitive information** and have access to this information locally on the device.

A significant amount of **corporate** data can be found **locally on user devices**.

IT needs to be able to **secure, classify, and protect data** based on the content it contains, not just where it resides, including **maintaining regulatory compliance**.

Solutions

Users can work **on the device of their choice** and be able to access **all their resources**, regardless of location or device.

IT can enforce a set of **central access and audit polices**, and be able to protect sensitive information **based on the content of the documents**.

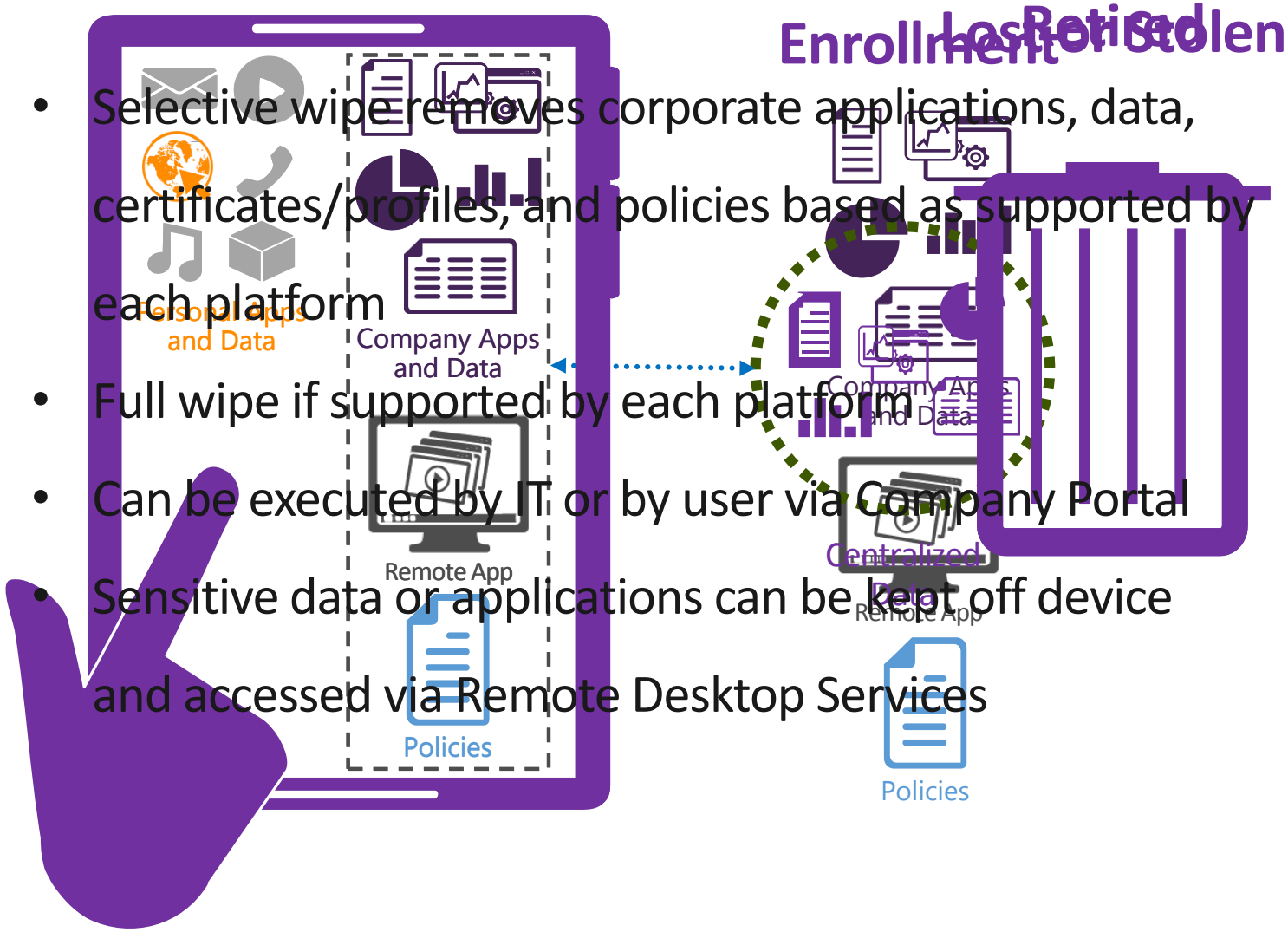
IT can **centrally audit and report** on information access.

Protect your data

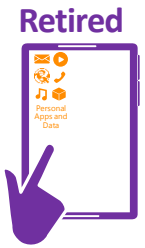
Help protect corporate information and manage risk

Users can access corporate data regardless of device or location with **Work Folders** for data sync and **desktop virtualization** for centralized applications.

IT can provide a secure and familiar solution for users to access sensitive corporate data from anywhere with **VDI** and **RemoteApp** technologies.



- Selective wipe removes corporate applications, data, certificates/profiles, and policies based as supported by each platform
- Full wipe if supported by each platform
- Can be executed by IT or by user via Company Portal
- Sensitive data or applications can be kept off device and accessed via Remote Desktop Services



Benefits of Unified Device Management

- Lower TCO – Lower provisioning costs by provisioning OTA, Self service portals lower IT administrative overhead
- Improved ROI – Achieving more with less (reusing same resources for MDM)
- Reduce Complexity – One single pane of administration, no additional know how required, no additional infrastructure to be installed
- Increase Security - Secure enterprise app store, multi-factor authentication, auto VPN on demand, integration to local PKI and VPN solution (Juniper Pulse, Cisco AnyConnect, Dell SonicWall, F5 Edge Client, Checkpoint Mobile VPN, etc.)

Benefits of Unified Device Management

- Improve Employee experience – BYOD enablement, Single sign on for all services, acces to relevant apps/data at all times, ability to sync data on various devices pc & mobile
- Reduce Liability and legal Concerns - Lock and wipe devices if lost or stolen remotely, once an employee leaves the company they would no longer have access to sensitive information
- Improve Customer experience - external sales agents can service customers better on site due to access to relevant apps and data on both PC & Mobile

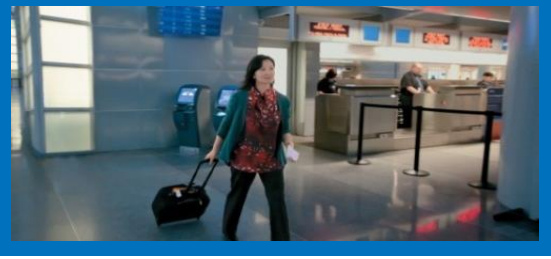
Benefits of Unified Device Management

- Improve Support – Self service portals fit new end user paradigm
- Increase Productivity and efficiency – Mobile integration and syncing of data on all types of devices mobile and fat clients
- Provide Greater Choice – Customer can choose on premise, cloud or hybrid model
- Offer attractive pricing – No maintenance charges, no hidden costs, simple user subscription as an add on to Core CAL

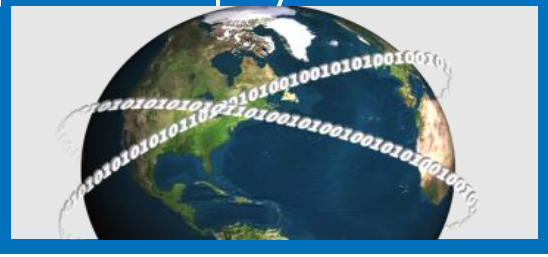
Windows Intune Key Customer Scenarios

Mobile Devices

Remote Workers



Application Deployment to Devices



Quick Deployment Scenarios

Key Takeaways

- Unified Device Management enables lower TCO with lowest risk
- One solution including MDM, MAM, MEM and PC Management
- Commercially attractive with user based subscription model with no additional mantainence charges or hidden costs
- For additional information please contact me at ankhan@microsoft.com

Q& A