People-centric IT

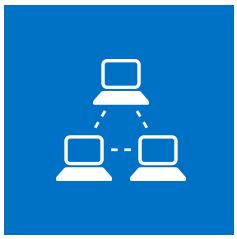
Top 10 Customer Benefits

Enterprise users can empower productivity with device choice through Microsoft solutions, providing IT professionals with a unified environment for managing all PCs and devices. With IT in control with a central, integrated system, they can ensure that end users have the applications they need on the devices of their choice. The Microsoft solution also enables IT to classify and further protect your data to meet compliance and security requirements.

Enable end users

1. **Simplify registration and enrollment for Bring Your Own Device programs (BYOD).** Users can manage their devices as well as install corporate apps through a consistent company portal.
2. **Access company resources consistently across devices.** Users can work from the device of their choice to access corporate resources regardless of location.
3. **Support modern work styles.** Microsoft Virtual Desktop Infrastructure (VDI) enables IT to deliver a corporate desktop and applications to employees that can be accessed from personal and corporate devices, from both internal and external locations, with the infrastructure running within the corporate datacenter.
4. **Connect automatically to internal resources when needed.** Users can connect to corporate resources with automatic VPN connections.

Unify your environment



5. **Access on-premises and in the cloud resources with common identity**. IT can better protect corporate information and mitigate risk by being able to manage a single identity for each user across both on-premises and cloud-based applications.
6. **Unify management of on-premises and cloud-based devices.** IT can extend its System Center Configuration Manager infrastructure with Windows Intune to support cloud management of devices with a single administration console, where applications can be deployed to users across all their devices.
7. **Provide comprehensive settings management across platforms.** Policies can be applied across various devices and operating systems to meet compliance requirements. IT can provision certificates, VPNs, and Wi-Fi profiles on personal devices within a single administration console.

Protect your data

8. **Protect corporate information with remote data and application control**. IT can access managed mobile devices to remove corporate data and applications in the event that the device is lost, stolen, or retired from use.
9. **Deliver policy-based access control to corporate applications and data.** IT can set policy-based access control for compliance and data protection.
10. **Enable selective wipe for lost or stolen devices.** IT can selectively and remotely wipe a device, including removing applications and data, management policies and networking profiles. Users can selectively wipe corporate applications and data from their devices.

Microsoft

Top 10 Benefits and Features

Empower users

	Benefit	Description	Product/Feature
1	**Simplify registration and enrollment for Bring Your Own Device programs (BYOD)**	Microsoft is making it easier for organizations to allow people to use the devices they choose by enabling those devices to be integrated into the security and management models IT may already have in place. **Users can register their devices in order to gain access to corporate resources, then manage their devices as well as install corporate apps through a consistent company portal** Supporting BYOD in the workplace requires a simple way for users to register their devices for use and ways to enable IT to manage those devices as part of the corporate infrastructure. Workplace Join in Windows Server 2012 R2 enables IT users to register their devices in Active Directory, and IT can require multi-factor authentication as part of this process. Additionally, users can enroll their devices for management, which joins the devices to Windows Intune and allows the installation of the company portal.	Windows Intune System Center Configuration Manager 2012 R2 Windows Server 2012 R2: Active Directory (R2 Schema) ADFS Web Application Proxy (for external) Windows 8.1 and iOS (at GA)
2	**Access company resources consistently across devices**	Microsoft enables IT to make corporate resources available to people on the devices of their choice from virtually anywhere, while enforcing security policies and retaining control for corporate compliance. When a user enrolls a device for management, the company portal is installed on the device. This company portal is consistent across devices, and it makes the latest corporate applications available to users. Work Folders, new in Windows Server 2012 R2, enable users to store the data they need for work in one place and make it easy for users to sync this data across devices.	Windows Server 2012 R2: Remote Desktop Services Work Folders
3	**Support modern work styles**	Microsoft VDI enables IT to deliver desktops and apps to users on a range of devices. VDI maintains storage and compute in the datacenter, so the integrity of the data is always maintained and mitigates the risk of losing data on stolen or lost devices, while also providing business continuity by making the desktop available from anywhere. Microsoft VDI provides efficient management and a rich user experience at the best value for VDI.	Windows Server 2012 R2: Remote Desktop Services
4	**Connect automatically to internal resources when needed**	Microsoft provides the ability for corporate resources to be available to users on the devices they use, removing the complexity of configuring the devices and enabling IT to enforce who and which devices can access corporate resources. **Users can connect to corporate resources with automatic VPN connections.** Security features that help automate user access to resources include: DirectAccess provides an "always on" connection for domain joined Windows clients; the Remote Access role in Windows Server provides traditional VPN connections from user devices to corporate resources; the Web Application Proxy allows IT to publish access to corporate resources; and new in Windows Server 2012 R2 we provide the ability for applications to trigger the VPN on the user's behalf as they are launched.	Windows Server 2012 R2: DirectAccess & VPN Web Application Proxy Windows 8.1 Windows Intune (MDM devices)

Unify your environment

	Benefit	Description	Product/Feature
5	**Access on-premises and in the cloud resources with common identity.**	A paramount concern of any IT department is protecting he security of corporate resources. Every time a user attempts to access data, it creates a potential security risk. Managing the risks associated with how people work was simpler when they accessed corporate resources using only corporate-owned and managed assets. Security becomes far more complex as enterprises move to a people-centric model in which corporate resources can be accessed using either corporate –or employee-owned devices of any type.	Windows Server 2012 R2: Active Directory Windows Azure Active Directory

Microsoft

		Microsoft recognizes the need to provide more secure access to sensitive corporate resources when they're consumed on BYO devices. Windows Server Active Directory and Windows Azure™ Active Directory provide functionality that enables IT security administrators to manage a person's identity regardless of whether the resources the person is accessing are on-premises, in the cloud or from external networks.	
6	**Unify management of on-premises and cloud-based devices.**	IT can extend its System Center Configuration Manager infrastructure with Windows Intune to support cloud management of mobile devices. This unified management enables IT to publish corporate apps and services across device types, regardless of whether they're corporate-connected or cloud-based. Microsoft provides a unified way for organizations to view and manage all the devices accessing corporate resources, including Windows-based PCs, tablets, phones, and servers, Windows Embedded devices, Macs®, iOS® and Android™ smartphones and tablets, as well as UNIX®/Linux® servers. This integration means that organizations don't need to learn or implement different, segregated products.	Windows Intune Configuration Manager
7	**Provide comprehensive settings management across platforms**	Policies can be applied across various devices and operating systems to meet compliance requirements, and IT can provision certificates, VPNs, and Wi-Fi profiles on personal devices within a single administration console Together, System Center 2012 R2 Configuration Manager and Windows Intune provide organizations with a holistic view of all devices accessing corporate resources, whether they're PCs or mobile devices, on-premises or in the cloud. IT can define security and compliance settings to help ensure that devices accessing corporate resources meet corporate policies.	Windows Intune Configuration Manager

Protect your data

	Benefit	Description	Product/Feature
8	**Protect corporate information with remote data and application control.**	As people lose or upgrade their mobile devices, or if they no longer work for the organization, it's crucial to make sure that any corporate-related information, including applications and data, are no longer available on their devices. With System Center 2012 R2 Configuration Manager and Windows Intune, corporate resources can be remotely removed from the device by either the user or IT, while the personal data on the device is left alone.	Windows Intune Configuration Manager
9	**Deliver policy-based access control to corporate applications and data.**	Windows Server 2012 R2 gives IT the ability to make sensitive corporate information available to users, while retaining control over which users and devices can access the information through the enforcement of conditional access policies. Windows Server 2012 delivered a new solution, Dynamic Access Control, which allows IT to configure content classification policies, along with dynamic conditional access policies and actions based on the outcome of the classification process, such as automatically encrypting documents using Rights Management Services. With Windows Server 2012 R2, IT can now publish access to corporate resources using the Web Application Proxy and enforce conditional access policies with multi-factor authentication. IT can also enable users to sync their files to their devices using Work Folders, and this includes integration with the Dynamic Access Control policies.	Windows Server 2012 R2: Dynamic Access Control Rights Management Services Active Directory ADFS Web Application Proxy (external)
10	**Enable selective wipe for lost or stolen devices.**	With System Center 2012 R2 Configuration Manager and Windows Intune, mobile devices can be selectively wiped to protect corporate data and applications. These Microsoft tools also provide a way for people to retire a device when they no longer use it to access corporate resources. IT can selectively and remotely wipe a device, including removing applications and data, management policies and networking profiles. Users can selectively wipe corporate applications and data from their devices.	Windows Intune Configuration Manager

Microsoft