Microsoft

Access and Information Protection

Enable Users, Protect Your Data

Users

- Demanding their own choice of device
- Wanting anywhere connectivity

IT

- Incorporating BYO devices while maintaining compliance and data protection

Facts

- Worldwide total unit shipments for smart connected devices will reach 1.2B in 2012 and grow 16% to over 2B units in 2016.[1]
- According to a Forrester 2012 report, enterprises now list mobile and app security among their highest priorities, with 46% indicating that improving or implementing mobile security is a 'high' priority over the next 12 months. Another 22% deemed this move to be 'critical'.[2]
- Only 30% of firms have policies and sufficient tools for employee-owned smartphones; 15% lack a policy entirely. [3]

The challenges

- Users want consistent access to corporate services wherever they are, on any device.
- Businesses need to effectively manage the influx of consumer devices while continuing to deliver on operating efficiency and without compromising data.

Access and Information Protection – A Windows Server 2012 R2 Story

- Simplified registration and enrollment for unmanaged and BYO devices
- Automatic connections to internal resources when needed
- Access to company resources remains consistent across devices
- Common identity to access resources on-premises and in the cloud
- Centralized corporate information for compliance and data protection
- Policy-based access control to applications and data

Access and Information Protection

Windows Server 2012 R2 Access and Information Protection solutions provides your users with secure access to corporate resources from virtually anywhere, enabling them to work productively on the device of their choice. Taking advantage of existing investments in Active Directory and connecting to Windows Azure Active Directory, Windows Server 2012 R2 provides IT with the ability to federate a user's identity with Windows Azure and other cloud-based identity domains. Users get a common identity to access resources on-premises and in the cloud, enabling them to sign on once to gain access to all their applications and data.

Windows Server 2012 R2 also provides a mechanism to register unmanaged and BYO devices in Active Directory, making devices known to IT so that they can be taken into account as part of conditional access policies. This enables the user to gain access to corporate resources. Users can also enroll their devices with the Windows Intune management services, enabling them to use the Company Portal that provides a consistent experience to access applications, data, and self-service device management. Windows Server 2012 R2 Remote Access with Windows 8.1 can automatically connect to internal resources when needed with an automatic VPN connection. Additionally, users have the ability to access their work documents consistently across devices by using Work Folders, a new sync capability in the File Server role.

To protect corporate data, Windows Server 2012 R2 lets IT centralize corporate information for compliance and data protection. Moving data from unmanaged decentralized locations such as laptops into a managed location and then enabling data sync to devices achieves the dual goals of letting IT gain control of information and users to work the way they want. Policy-based access control to applications and data takes into account the user's identity, if the user's device is "known" (registered), and the user's location (internal or external to the corporate environment).

Whether you are an enterprise, a service provider, or a small or medium-sized business, Windows Server 2012 R2 can help you optimize your business.

[1] IDC Press Release, IDC Expects Smart Connected Device Shipments to Grow by 14% Annually Through 2016, Led by Tablets and Smartphones September 26, 2012

[2] Benchmarking Your Enterprise Mobile Device Operations Initiatives And Plans, Forrester Research, Inc., October 10, 2012

[3] 'Mobile Workers Use Personal Apps to Solve Customer Problems—Is It Ready, Willing, and Able to Assist? A September 2012 commissioned study conducted by Forrester Consulting on behalf of Unisys'

Published, October 1st, 2013

Enable Users

Windows Server Remote Access	Enables users to work remotely and stay connected to the corporate network without initiating a VPN connection with DirectAccess. Remote Access also provides automatic VPN connections when a user launches an application that requires access to corporate resources.
Web Application Proxy	Enables IT to publish access to resources based on device awareness and the user's identity. Through integration with AD FS, IT can also pre-authenticate the user and the device and enforce access policies such as requiring the device to be registered or invoking multi-factor authentication.
Workplace Join	Makes unmanaged and BYO devices known to IT; enables single sign-on and gives access to corporate data; puts a certificate on the device and registers a new device record in Active Directory.
Work Folders	Enables users to securely sync their data from corporate File Servers to all of their client devices (and vice versa); ensures that a copy of the data is kept within the corporate realm so that it's available, backed up, and subject to corporate business rules with Dynamic Access Control and Rights Management.
Device enrollment	Configures the device for management with Windows Intune. The user can then use the Company Portal for easy access to corporate applications.
Windows Azure Mobile Services	Helps developers integrate and enhance their applications with a number of capabilities that speed up the development process such as linking to data sources, authentication, and configuring push notifications.
Enhanced Active Directory Federation Services	Offers enhanced BYO device support including registration service for consumer devices to drive conditional access, device authentication, conditional access, and modern LOB applications.

Hybrid Identity

Identity management	Utilizes Active Directory Federation Services to connect with Windows Azure for a consistent cloud-based identity. Users can take advantage of their common identity through accounts in Windows Azure Active Directory to access Windows Azure, Office 365, and 3rd-party applications.
Virtualization support	Enables IT to run Active Directory at scale with support for virtualization and rapid deployment through domain controller cloning.

Protect your data

Multi-factor authentication	Utilizes integration with Windows Azure Multi-Factor Authentication to enable IT to enforce multi-factor authentication when users connect.
Dynamic Access Control	Enables the automatic identification and classification of data based on content. Integration with Active Directory Rights Management Services provides automated encryption of documents. In addition, IT can apply central access and audit policies across multiple file servers, with near real-time classification and processing of new and modified documents.
Selective wipe	Wipes corporate data from a device in the event that the device is lost, stolen, or otherwise needs to be decommissioned.

Download and Trial Windows Server 2012 R2
www.microsoft.com/en-us/server-cloud/windows-server

Learn more about the Access and Information Protection Solutions
www.microsoft.com/en-us/server-cloud/solutions/access-information-protection.aspx

Published, October 1st, 2013

Microsoft