Microsoft

Hybrid Identity

Contents

Introduction

This paper presents an overview of Microsoft's approach to identity as part of the People-centric IT vision—how we help businesses address some of the top IT challenges arising from the consumerization of IT and the movement to the cloud.

Microsoft's identity solutions span on-premises and cloud-based capabilities, creating a single user identity for authentication and authorization to all resources, regardless of location. We call this *Hybrid Identity*.

Today's challenges

Simply put, the biggest IT identity challenge we face today is keeping users productive while protecting company information. This challenge arises from several new pressures.

The explosion in the use of consumer devices and the ubiquitous access to information is changing the way people perceive their technology, and how that technology shapes their lives, both at home and at work. In fact, the traditional separation between "personal life" and "work life" is now blurred by the constant use of IT throughout the day and easy access to information in most locations. The shifting boundaries are accompanied by a belief that personal technology—selected and customized to fit the user's personalities, activities, and schedules—is as much part of "work" and the workplace as it is the rest of life.

Historically, most or all devices used in the workplace were owned and therefore managed by the organization. Policies and processes focused on device management—and usually on a relatively small, tightly controlled and managed set of corporate-approved hardware that was replaced on a predetermined corporate cycle.

The consumerization of IT dramatically alters this scenario. There are more devices in the organization, and those devices run a much more diverse set of operating systems and software. This is a fundamental change in the IT landscape and requires a shift in management objectives: Instead of striving for tight control over hardware, organizations need effective governance that is centered on the users, not the hardware.

The way users access resources and applications is also changing. With the shift to personal devices and mobility, applications are also changing. Choices need to be made about which platforms will be

supported for each application. Alternatives may need to be investigated, such as desktop virtualization. Maybe it's time to migrate some applications into modern service-orientated web applications. Microsoft's customers must also now consider authentication of the user, validation of the device, and updated service consumption models when planning policies and implementation.

In the optimal scenario, IT policies match business realities and priorities and are based on people, not only on device management. The Microsoft People-centric vision helps IT administrators increase productivity by enabling access to corporate resources, regardless of location or device used.

Leading in this new era requires policies, processes, and technologies that give people the freedom to select the devices they want to use as well as support for device-agnostic access to applications and data.

Microsoft's approach

Microsoft has a history of providing rich IT infrastructure solutions to help manage every aspect of enterprise operations. Now, Microsoft's products, technologies, and services combine to create a people-centric solution that can help IT departments handle the influx of consumer-oriented technology and the work style expectations of users, thereby helping increase productivity and satisfaction for the people within their organizations.

The People-centric vision is being realized in three broad areas:

- Unifying your environment
- Enabling your end users
- Protecting your data

Each of these areas is covered more completely later in this paper, but here is an overview to get started.

Unifying your environment

Unifying your environment means delivering comprehensive management of users, devices, and applications found both on-premises and in the cloud. You can leverage your existing on-premises infrastructure, including Microsoft System Center Configuration Manager, Windows Server, and Active Directory Domain Services (AD DS), as well as cloud-based services, including Windows Intune and Azure Active Directory.

Key to meeting this vision is having a common identity for users, along with a unified way to manage user identities for IT. Even in cases where

the systems require multiple identities, they are managed together, synchronized, or federated so that the user sees them as one.

The user's common identity can then be used to access resources on-premises and in the cloud. This unified environment leverages the existing investments that organizations have in AD DS, and can connect to Azure AD to provide the ability to federate identities between AD DS and Azure AD and other cloud-based identity domains.

Enabling your end users

You can enable your end users by allowing them to work on devices of their choice and providing consistent access to corporate resources from those devices. From the users' point of view, this is no more and no less than letting them get their job done.

Windows Server 2012 R2 provides the ability for users to register their devices to access corporate resources, and then enroll their devices with the management services to use the company portal for access to applications and to manage their devices. Windows Server 2012 R2 also lets users synchronize corporate data to their device using Work Folders.

Azure AD is an identity and access management platform for cloud services and applications. It provides identity capabilities (including single sign-on [SSO]) for cloud applications such as Office 365 and other Software as a Service (SaaS) applications. Features such as Self-Service Password Reset, Group Management, and Multi-Factor Authentication (MFA) provide customers with powerful ways to authorize and authenticate users for access to their cloud applications, all integrated with existing on-premises investments in AD DS.

Protecting your data

To properly protect your data, you must secure corporate information and manage risk, including following corporate policies, compliance directives, regulations, and laws. However, users want to be able to access their information on the devices that they bring into the corporate world.

Several approaches exist to achieve this somewhat dichotic goal, and both approaches are enabled by features in Windows Server 2012 R2.

One approach is to 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 keeps corporate control of company information but also enables users to work the way they want.

Another approach is to create policy-based access control to applications and data, taking into account the user's identity, whether

the user's device is known (i.e., registered), and also the location—internal or external—from which access is requested.

New cloud capabilities such as Azure Rights Management Services enable customers to protect data at the document level, whether that data be at rest, in transit, or being opened or edited across all document types and platforms. Developers can build native applications that integrate this capability, building a rich ecosystem in which customers can protect data from any applications on any platform.

The rest of this paper examines each of these three pillars in more detail as they relate to Hybrid Identity and focuses on solutions provided by Microsoft's on-premises and cloud-based technologies, features, and services.

Unifying your environment

Delivering comprehensive management of users, devices, and applications requires a consistent view of user identity, and that view must stretch across your on-premises installations, your cloud apps and services, public SaaS apps, and even business-to-business (B2B) interactions with federated partners.

As with users blending their work and personal lives, companies are looking to blend their existing on-premises applications to take advantage of new cloud-based services. When this happens, you must find a way to consistently manage identity. Microsoft software and services support a Hybrid Identity model that allows for coexistence between on-premises infrastructure and the cloud as well as a traditional on-premises model or a cloud-first model that relies little (or not at all) on on-premises data.

Generally, organizations start by leveraging their existing investments on-premises and connecting out to cloud-based services. This allows users to be as productive as possible, with SSO to all their resources. A common identity can be used across on-premises or cloud-based services by beginning with Windows Server AD DS, and then connecting to Azure AD.

On-premises, centralized identity

Creating a strong, reliable, centralized identity usually begins with the on-premises resources that an organization already holds and uses.

The core of a Microsoft-based centralized identity is Active Directory. AD DS is already in place in many organizations, so start with what you have. To centralize disparate sources of user properties, profile information, and authentication stores, you can use Microsoft Forefront Identity Manager (FIM) 2010 R2. FIM is discussed in more detail later in this paper, as it also provides self-service abilities to enable users to be more productive.

Going beyond on-premises

Most organizations will not remain completely on-premises for much longer. Some organizations, particularly those without a large investment in on-premises AD DS, are already beginning to adopt a cloud-first strategy in which cloud-based authentication is the default authentication method or in perhaps the only authentication method in use.

IDC predicts that 70 percent of chief information officers (CIOs) will embrace a cloud-first strategy by 2016, but to get there, organizations need to move at their own pace over a number of years, with many living in a hybrid environment for quite some time. That flexibility—living in both worlds—even with a cloud-first strategy, is non-negotiable.[1]

This means that each organization has to choose an approach or combination of approaches to follow. Approaches may include:

- **Cloud identity (cloud-first strategy).** All identity resides in the cloud.
- **Identity Sync.** Identity information is kept in sync between the existing on-premises infrastructure and the cloud. With AD DS and Azure AD, the synchronization may include full credentials or only some information.
- **Federated identity.** Authentication for cloud apps is performed on-premises using SSO and federation.
- **B2B federated identity.** This approach allows business partners to securely share and collaborate by being able to authenticate users from the other partner.

The next few sections of this paper examine some of these possibilities in greater detail.

[1] Source: IDC CIO Agenda Webinar, 2013.

Sync with the cloud

The first step in bridging identity between on-premises AD DS and Azure AD is to implement a synchronization engine. Historically, this has been performed by a tool known as the Directory Synchronization Tool (DirSync), which synchronizes one AD DS domain with Azure AD. Microsoft has now released a new sync engine, Azure Active Directory Sync Services (Azure AD Sync). Azure AD Sync handles the simple one-to-one model of DirSync as well as complex AD DS sync scenarios, such as multiple domains and forests, and other identity stores, such as Lightweight Directory Access Protocol (LDAP), generic SQL via ODBC, web services (e.g., SOAP, Java, and REST), and Windows PowerShell.

Azure AD Sync does all of this in the free version, but with a subscription to Azure AD Premium, Azure AD Sync will also perform a write-back of attributes from Azure AD to an on-premises directory. When writing back to AD DS, we can sync users, groups, devices, and passwords additionally.

Both of these synchronization engines support *full sync,* where the users' password hashes are synchronized, or *federation,* where the password hashes are not synchronized and all authentication is passed back and performed in the on-premises AD DS forest (Figure 1).

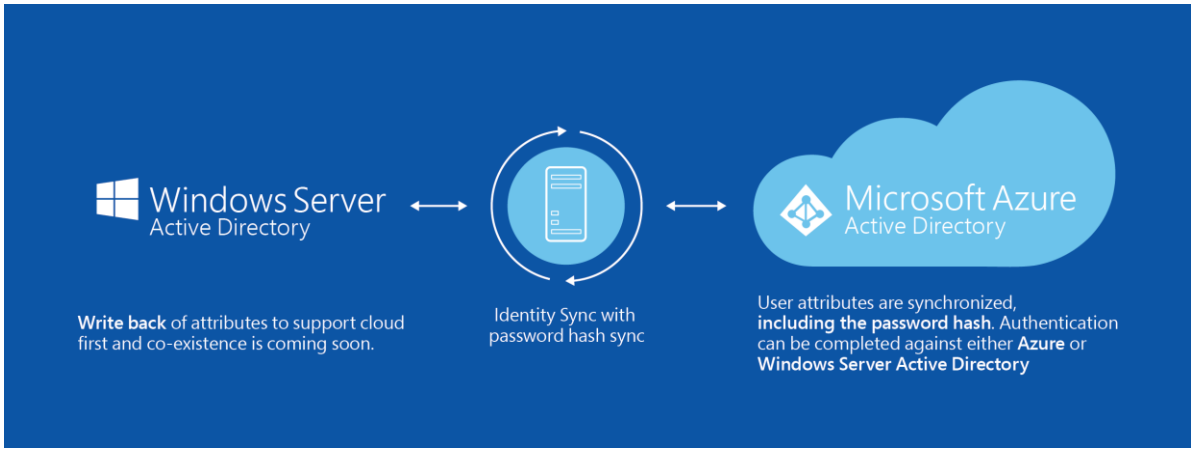

Figure 1. Authorization through synchronization

Azure AD now supports Multi-Factor Authentication (MFA) integrated with Active Directory Federation Services (AD FS) when federated with an on-premises AD DS infrastructure. A more detailed description of Azure MFA follows later in this paper.

Until now, changes to user attributes had to be made at the on-premises AD DS, and then synchronized "up" to the cloud. With the introduction of write-back, changes can now be made in the cloud, and then sent to the on-premises AD DS forest. For organizations where many users are mobile or where users tend to access services primarily through the cloud, this increases flexibility and responsiveness.

Another improvement that supports a cloud-first viewpoint is the ability to synchronize from different databases directly to Azure AD without first having to go through AD DS using Azure AD Sync. This is shown in Figure 2.

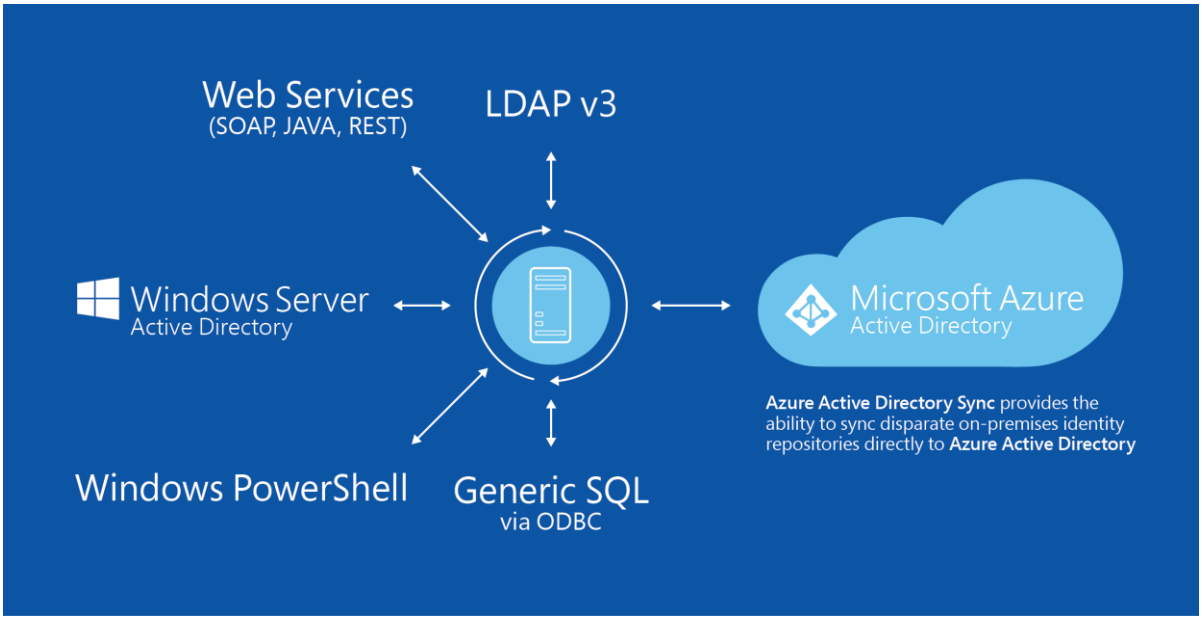

Figure 2. Synchronizing databases through Azure AD

User attributes stored in LDAP repositories, web services, Windows PowerShell, and generic SQL via ODBC along with those from AD DS can be synchronized with Azure AD in the cloud directly. Customers who want to sync these repositories purely on-premises can use FIM Sync.

Federation with the cloud

If you prefer that authentication occurs against your on-premises AD DS infrastructure, you can deploy AD FS for federated authentication with the cloud. AD FS simplifies end user access to systems and applications by using a claims-based access authorization mechanism to maintain application security.

A sync engine is used to replicate user attributes to Azure AD but without synchronizing the password hashes. Instead, authentication is passed back to the on-premises AD DS infrastructure via federation, and it is the on-premises AD DS forest that performs the authentication. In this case, AD FS can be configured, if desired, for MFA on a per-application (relying party) basis. In addition, AD FS can leverage device registration (Workplace Join) or other claims that the user presents.

When this single identity has been established, users can connect to SaaS applications running in Azure or Office 365 and from non-Microsoft providers, offering users an SSO experience. Azure AD

currently has more than 1000 applications that can be configured for SSO, and the number continues to grow. In addition, organizations can federate with business partners and other organizations for seamless access to shared resources in the B2B federation model.

Figure 3 represents the cloud federation model.

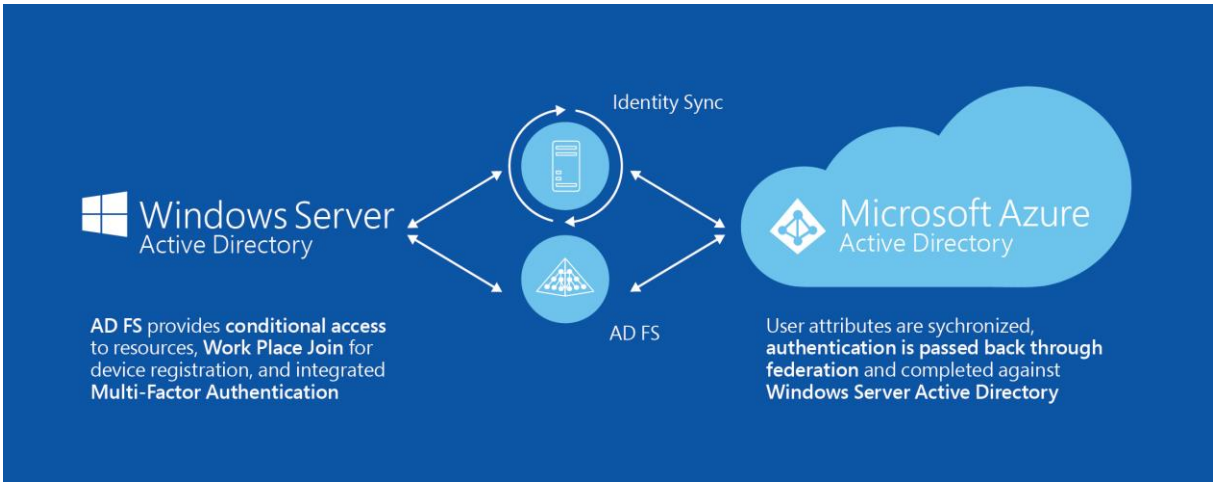

Figure 3. The cloud federation model

Building a common identity with Azure AD

Azure AD is more than a "domain controller running on a cloud-hosted server," and more than a directory in the cloud. It is an Identity and Access Management Solution as a Service.

Azure AD offers several capabilities that can allow customers to expand their identity footprint from on-premises into the cloud:

- Synchronizing with AD DS, as described earlier
- Federating with AD DS, as described earlier
- Cloud-Only Authentication
- Pre-integrated SaaS apps for SSO and allowing corporate credentials to "just work"
- Custom line-of-business (LOB) app support and developer features
- User self-service capabilities like password reset and group management

By using Azure AD, your organization will be well positioned to adopt cloud-first or Hybrid Identity scenarios.

Cloud-Only Authentication

Azure AD can provide identity management for cloud-only solutions. To provide a custom-branded cloud directory that will host identities and provide authentication to cloud-based apps (whether built on Azure or on any other public cloud), create an Azure AD tenant, name it, add users, and assign to them access to the cloud-based apps. They will have a new set of credentials (not a Hybrid Identity SSO) that will work with the selected apps and nowhere else.

This model works well for one-off customer–partner-vendor projects for new companies or public-facing projects that are cloud based and do not have (and may not want to have) an on-premises infrastructure.

Pre-integrated SaaS apps

Microsoft has worked with the most popular cloud applications, regardless of which public cloud provider hosts them, and preconfigured all the parameters needed to integrate or federate with each of them. Microsoft created an application gallery that presents all of the pre-integrated apps. Simply choose those that your enterprise uses, and you can easily configure SSO for each app. This SSO may be a native federation, or it may leverage password vaulting when federation is not available.

This pre-integration and SSO for SaaS apps also allows specific corporate users to sign on to your company's account with these applications without knowing the underlying password for the account, using only their corporate credentials. Not only is this highly convenient, but it also helps protect your company account from rogue access, terminated employees, or leaked passwords.

In the application gallery, you can find apps from Microsoft and other publishers. Examples include Office 365, Windows Intune, Salesforce.com, Box, Google Apps mail, and Concur, with more being added frequently. Figure 4 shows a sampling of apps available in the Azure AD Application Gallery.

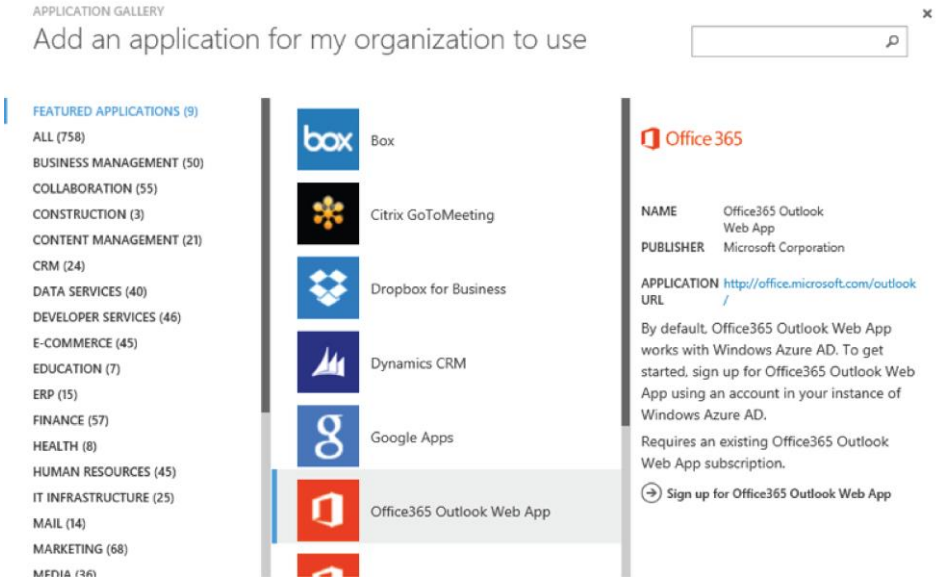

Figure 4. Apps available in the Azure AD Application Gallery

Custom LOB app support and developer features

If your enterprise uses cloud-based SaaS or custom LOB applications that are not pre-integrated into Azure AD, you can follow simple steps to add them and enable SSO to them, as well.

Azure AD provides a way for developers to integrate identity management into new apps. An application can be built on any platform—Microsoft .NET, Node, Java—and be hosted in any cloud, with Azure AD handling the identity management.

Azure AD Graph API allows an app to query the directory and receive a view of the enterprise directory and the relationships among its objects for use in the application. For example, if an application has a workflow that must include the manager or the team of a user, the developer can retrieve their identities through Graph API.

Workload example: Office 365 and Windows Intune

Contoso, Ltd., has been a growing business for many years. Based in the western United States, new opportunities have opened up across North America. To meet demand, Contoso has had to add new staff, almost doubling the number of employees in less than a year. Many of the new staff are working remotely, and Contoso is investigating opening two new branch offices for sales and support in their new territories.

Contoso has had an on-premises IT department with minimal staff. Until recently, the company has maintained an in-house AD DS infrastructure with two domain controllers. Most long-term users have desktops or laptops with Microsoft Office installed, using Microsoft Outlook to connect to an on-premises Microsoft Exchange Server instance.

The increases in staffing levels is putting strain on IT resources. It has become difficult to manage and provision the computers that are not often connect to the office LAN, and extending the LAN and Active Directory to the branch offices is raising issues of complexity and cost.

Contoso decided to implement two products to increase its agility and support unpredictable growth. New users are being provisioned with Office 365, allowing them to install Office locally and work with documents securely in the cloud. Windows Intune is now being deployed across the company, beginning with new purchases, then existing laptops, and finally all other computers. Windows Intune allows the IT staff to monitor, manage, and maintain all Contoso computers, no matter how they are connected.

To provide a unified environment, Contoso is taking the following steps:

- Contoso is subscribing to Azure AD Premium to take advantage of all the offered services. Contoso management also believes that this will position the company well for future growth.

- Implementing Azure AD Sync, including password hashes and write back, allows users to authenticate either to the on-premises AD DS or to Azure AD in the cloud and ensures that the same credentials are valid for both scenarios.

- This combination also allows users to seamlessly access local resources, Office 365, and Windows Intune as well as files stored in OneDrive for business.

Summary

Many options and many choices offer flexibility to a wide variety of organizations. Generally speaking, as show in Figure 5, the following guidelines hold true:

- **Cloud Identity provides a single identity in the cloud.** This is well suited to small organizations that have no integration with on-premises directories. Larger organizations with public-facing projects may also choose this model for such projects.
- **Directory Sync.** This feature provides authentication on-premises or in the cloud and works well for medium-sized and large organizations that do not require or desire federation.
- **Federated Identity.** This feature provides a single, federated identity and credentials and works best in medium-sized and large organizations that need the benefits of federation and have the resources to manage it.

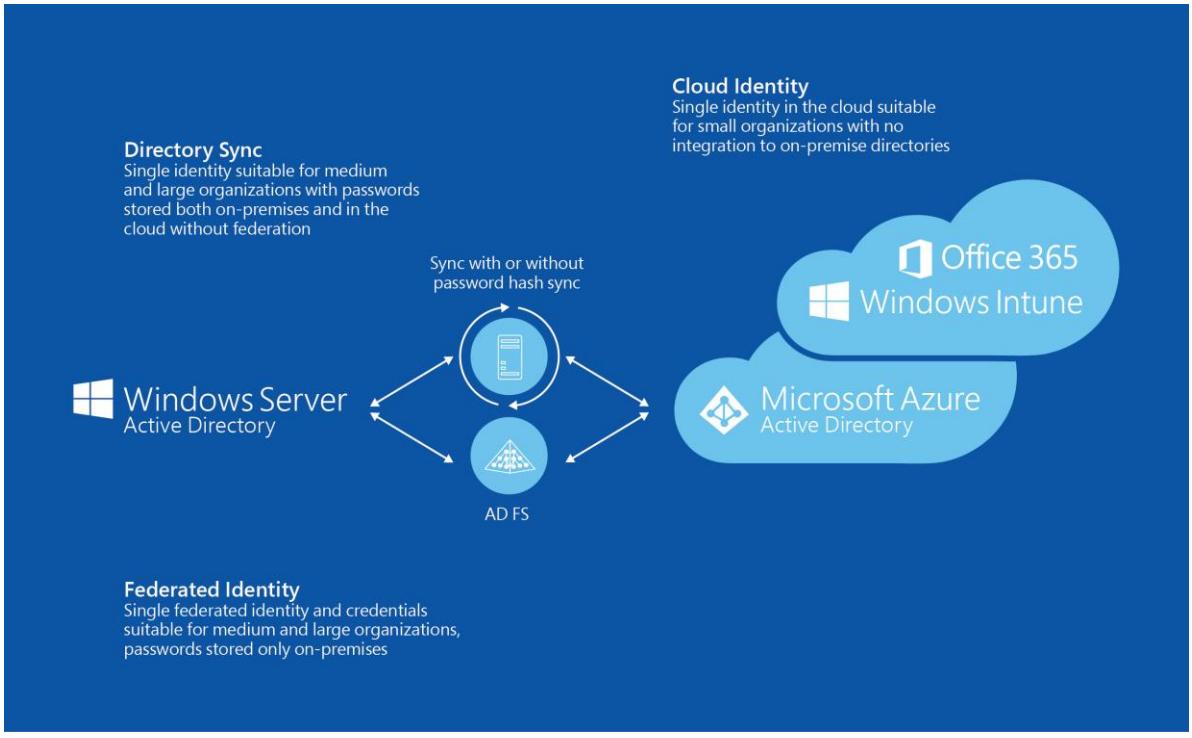

Figure 5. Today's authentication options

Enabling users

We need to make users productive through self-service and SSO experiences. To do so, two key scenarios must be implemented or enabled, namely:

- Self-service (either on-premises or cloud-based)
- SSO across all corporate resources

Self-service on premises

When users speak of *self-service,* they often describe it in terms of empowerment, satisfaction, and productivity. To an end user, *self-service* means getting things done immediately, without waiting and without a help desk call or having to follow a time-consuming process.

When self-service is effective, users say things like:

- I can request access to resources and applications.
- I can sign in to the applications I need with just one password.
- I get a familiar, personalized interface for things I need to do.
- I can get new team members up and running—with the right access—right when they start.
- I can change or reset my own password.
- I can edit my profile or directory information to correct errors or keep things up to date.
- I can manage my own groups for security or email.

These users use a lot of "I" statements, as illustrated in Figure 6, but they also reflect a desire for productivity and efficiency. They can sum up these statements with, "I am more productive!"

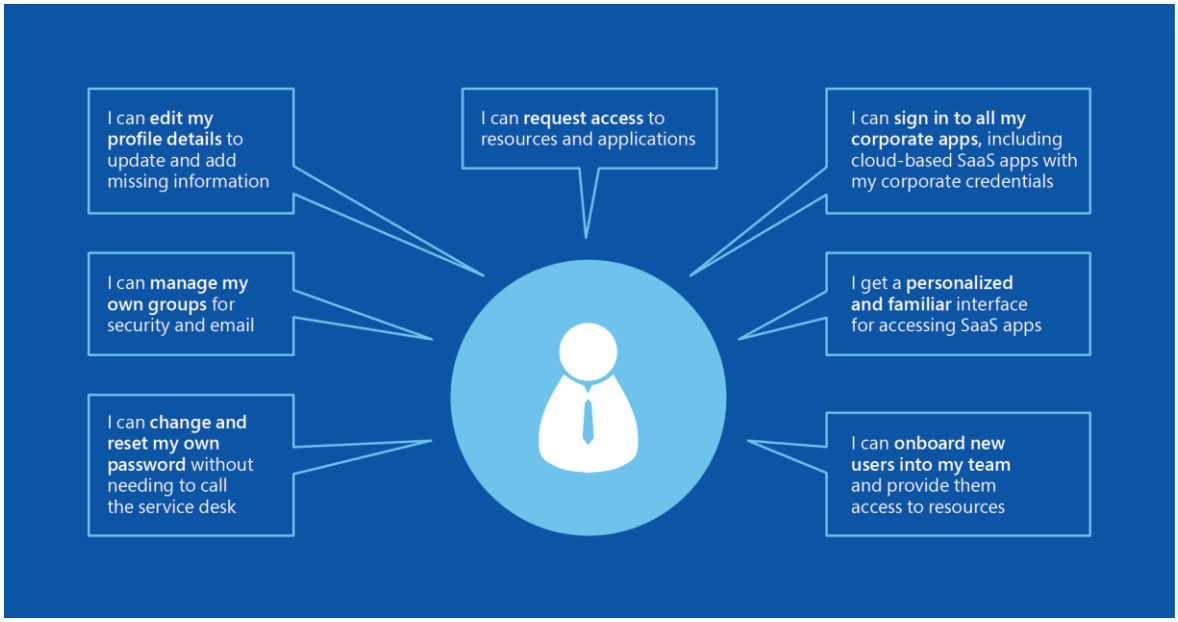

Figure 6: Self-service in a user-centric IT environment

Providing that empowerment, however, and managing users' identity often involve some complex tasks on the IT side. FIM 2010 R2 is the primary tool used to enable on-premises self-service, including:

- Self-service group and distribution list management, including dynamic membership calculation that is based on the user attributes in AD DS.
- Self-service password reset, which can significantly reduce help desk costs.
- Self-service identity management that allows users to manage their own attributes through an easy-to-use portal that is also tightly integrated with Office.
- Integration with AD DS to allow complete life-cycle management for Public Key Infrastructure (PKI) certificates and smart cards.
- Synchronization of users' identity across directories, including AD DS, generic SQL via ODBC, web services, Windows PowerShell, and LDAP data stores.

Self-service in the cloud

Users are already used to self-service models in the cloud, even more so than on-premises, simply because that has always been the model for consumer SaaS web applications. There is no way for the millions of users of popular services such as Outlook.com to have been provisioned individually by the teams operating those services. It is important, therefore, to extend the self-service model in the enterprise to cloud applications—both those operated by the enterprise and those SaaS apps that the enterprise uses.

By using Azure AD, you gain several self-service advantages:

- Users can reset their own passwords.
- Users can edit their profiles to add missing information, update with changes, or correct errors.
- Users can create and manage their own groups.
- The IT staff and authorized users can manage access requests for resources and group membership.

By connecting Azure AD in the cloud with your on-premises AD DS installation, you can leverage your existing investment and provide both cloud-based and on-premises users with a single set of AD DS credentials. In addition, users can use their AD DS credentials to access SaaS apps, such as social media sites, which they use on behalf of the company. These benefits are discussed later in this paper as part of the SSO experience.

Single sign-on

The term *single sign-on* can encompass several different scenarios, but the heart of the matter is that managing multiple sets of credentials—different user names with their accompanying passwords that must be changed on different schedules, smart cards, certificates, mobile authenticator apps, hardware dongles—is expensive and time consuming for the organization as well as frustrating and unproductive for the users.

The goal of SSO is to require the user to have only one set of credentials that can be used consistently across all systems and services—on premises or in the cloud—that the user needs to access. SSO does not prevent the use of MFA; rather, it enables it to be consistently applied when policy or regulation requires it.

SSO may allow users to seamlessly access additional services without presenting their credentials again, but at the least, it allows the same credentials to be used. From an IT point of view, this is typically achieved in one of two ways (Figure 7):

- The creation of a "metaverse" in which to store all information from all identity stores. This provides a singular view of the user across the entire environment. A sync engine keeps the passwords to all systems the same at all times.

- The use of a caching or vaulting solution presents the password to various systems on the user's behalf.

To the end user, the result is the same: one user name and password. To IT pros, these are very different things, with differing levels of complexity and configuration required.

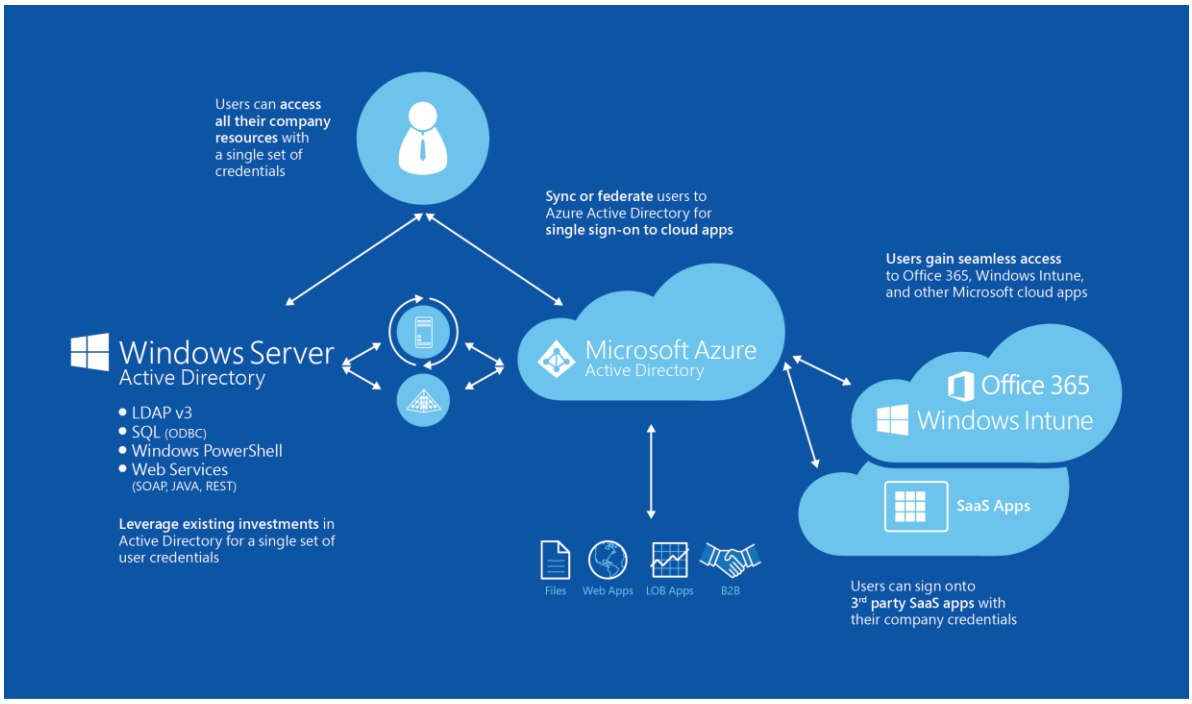

Figure 7. Accessing services through SSO

As shown in Figure 7, SSO may include the following:

- Users being able to access all company resources with a single set of credentials. This may require synchronization of user information between sources, such as LDAP repositories, databases in generic SQL via ODBC, and other mail systems.

- By synchronizing or federating between AD DS on premises and Azure AD, you can leverage your investment in AD DS and give users SSO to cloud apps.

- By adding AD FS, SSO scenarios can be established for connections to B2B service providers.

Workload example: SSO to SaaS apps

Contoso has established a social media presence to promote its products on many common websites. Each of these sites requires a user name and password that are used to post updates on behalf of the company. In some cases, employees also maintain their own "company-related" accounts to post more casual updates and build a conversation with their customers.

Management is concerned about the number of people who have access to the credentials used for the corporate posting and the lack of management around them. Recently, news media have covered several high-profile examples of unauthorized posts being made on behalf of companies, including at least one vendetta by a terminated employee. The IT department is also concerned about enforcing policies and keeping track of the various credentials in use.

Contoso has decided to use Azure AD to address these issues.

All of the social media sites authorized for use by Contoso are already included as preconfigured partners in the SaaS application gallery in Azure. Accordingly, Contoso took the following actions:

- The IT department changed the passwords for all company accounts on the social media sites, then used the Application Gallery to configure each company account.
- Authorized users were granted permission to post to the social media sites but had to sign on using their Contoso credentials. Doing so ensures that the underlying credentials for the site cannot be easily distributed.
- Contoso configured high-value accounts to require MFA, thus further limiting the risk of unauthorized access.
- The IT department recorded a simple video showing users how to connect their own company-related social media accounts to their AD DS account for SSO.

Protecting data

We need to balance our users' ability to work against business requirements, security, and compliance policies.

As users bring their own devices to work, they will need or want to access sensitive information, and sometimes they will require access to this information locally on the device. In this new world of consumerization, not only is data consumed or accessed on mobile and portable devices, but new data and updates are also created. This means that a significant amount of corporate data is likely to exist locally on user devices, and some of that data will be new and not yet exist anywhere else, like on a server.

The organization needs to be able to secure, classify, and protect data not based on where it resides but rather based on the content it contains, including maintaining regulatory compliance.

With services and software from Microsoft, including Windows Server 2012 R2 and the Azure cloud platform, you can allow users can work on the device of their choice, regardless of location, while still being able to enforce a set of central access and audit polices, protect sensitive information based on content, and centrally audit and report on information access.

Modern protocols: a summary

Many new and existing technologies and tools come into play when authenticating users and authorizing their access to data. To follow the complicated path that authentication and authorization can take, especially when involving the cloud or B2B scenarios, it is helpful to understand some of the key terms:

- **Security Assertion Markup Language (SAML).** SAML is based on XML and is used to exchange authentication or authorization data between two parties, usually an identity provider (or trusted party) and a service provider (or relying party). SAML is used extensively in many web-based SSO scenarios and also appears in other federated scenarios. AD FS uses and supports SAML.

- **OAuth.** OAuth is an open standard for authentication, mainly used when one user (or security principal) wants to grant another user or another service access to a resource under the user's control but without supplying his or her credentials (such as a password) to that other user. Many public SaaS websites, including several Microsoft sites, support OAuth.

- **Kerberos.** Kerberos is the primary authentication mechanism used within an AD DS forest. Originally developed at the Massachusetts Institute of Technology, it is now the Kerberos Consortium that promotes continued use and development of Kerberos. Microsoft is

a member of the Consortium. Other non-Windows systems also use Kerberos, some of which interoperate better than others.

- **Tokens.** In the context of authentication or authorization, a *token* is a piece of data, usually cryptographically signed, that contains or represents who a user is or what they are allowed to access. Windows builds a "security token" in memory whenever a user logs on to a computer or accesses a server. Software such as AD FS uses signed tokens in the SSO process. (In some contexts, *token* may also describe a physical dongle or device that the user must possess.)

- **Certificates.** Certificates are part of a PKI and are used to prove the identity of the certificate's "subject"—a server, computer, or user who is named in the certificate. A certificate includes a copy of the subject's public key that can be used to encrypt messages meant for the subject. The certificate is cryptographically signed by the certificate's issuing authority. If the system examining the certificate does not recognize the issuing authority, the certificate is not trusted and may not be accepted.

- **Cookies.** A *cookie* is data that is stored by a web browser. It is given to the browser by a website and is presented back to that website on subsequent visits or requests. Cookies may be temporary and kept only in memory (*session cookies*) or be persisted to disc. Many websites use cookies to "remember" who a user is and what they were doing on the site. In most SSO scenarios for the Web, cookies are used to store and pass tokens.

AuthN and access control

Today's organizations need the flexibility to respond rapidly to new opportunities. They also need to give workers access to data and information—across varied networks, devices, and applications—while keeping costs down. Innovations that meet these needs—such as virtualization, multi-tenancy, and cloud-based applications—help organizations maximize existing infrastructure investments while exploring new services, improving management, and increasing availability.

Although scenarios like hybrid cloud implementations, a mobile workforce, and increased work with non-Microsoft business partners add flexibility and reduce costs, they may also lead to a more porous or open network perimeter or even the inability to define the "perimeter" for company data. When organizations move more and more resources into the cloud and grant network access to mobile workers and business partners outside the firewall, managing security, identity, and access control becomes a greater challenge.

The latest version of AD DS supports data protection through robust authentication and access control. On premises, AD DS supports larger scale through easier virtualization and cloning options. Management tools have been improved and grown to include Windows PowerShell and the Active Directory Administrative Center (AD AC) for centralized management. AD AC centralizes management tasks into a single location, making it much easier to complete everyday administrative tasks against AD DS and associated features such as dynamic access control.

Azure AD and AD FS allow companies to reduce the infrastructure required on premises. In addition to Azure AD, Microsoft supports running domain controllers (AD DS) and AD FS on Azure (as Infrastructure as a Service), and those "cloud AD DS" infrastructure servers can be connected back on premises via the Azure Connect bridge. A number of deployment options with AD DS, Azure AD, and AD FS make it easier and faster to connect and authenticate cloud-based users, devices, and applications.

Developers can integrate applications for SSO across on-premises and cloud-based applications, providing a more productive experience for users and an easier way for customers to manage the identity of users within these applications.

Strong AuthN with certificates and MFA

Integration with Azure MFA provides IT with the ability to enforce MFA when users connect on a per-application basis.

When an application (or service) is configured for MFA, the application makes an MFA call when the user attempts to connect. The user must respond to the challenge, which can be configured as an SMS text message, a phone call, or a code generated using a mobile authenticator app. Only if a valid response is returned to the application is the user allowed to proceed.

Conditional access controls

Limiting access to corporate information can be challenging and costly. In Windows Server 2012 R2, Microsoft has made it easier to make information available to users while retaining control of how and where they can consume the information.

With Work Folders for data sync and desktop virtualization for centralized applications, users can access corporate data regardless of device or location. Work Folders allows the publishing and synchronization of data from inside the corporate boundary to client devices (and vice versa). When applications are not able or the organization does want them to be available locally on devices, desktop virtualization solutions allow users to work effectively. Users can access sensitive corporate data from anywhere with virtual desktop infrastructure and RemoteApp technologies without the risk of synchronizing that data to a mobile device.

Your company can publish resources by using the Web Application Proxy (a new role service within Remote Access that builds on the AD FS Proxy, with additional publishing capabilities) and create business-driven access policies with MFA based on the content being accessed. The Web Application Proxy is integrated with AD FS and therefore able to authenticate users and devices as well as make policy-based decisions on who and what can access information and enforce MFA on a per-application basis through the AD FS extensibility framework.

Even after users have been granted access, you can audit their access through central audit policies, configured and distributed through Group Policy.

Publishing

Making information and applications available to users when they are outside the corporate environment is challenging enough even when the devices being used are under full corporate control. When users start using their own devices, it introduces some additional considerations.

Commonly, AD DS remains the central repository of user identity and also holds the device registration information, storing not only the users' credentials but also the device information that can be used as part of the authentication process.

The Web Application Proxy (through the integration with AD FS) can authenticate users and devices, including the use of MFA. This means that as a user connects, they can be required to provide their basic identity credentials and also be required to pass additional credential challenges.

The Web Application Proxy consists of two services: a generic reverse-HTTPS proxy for publishing applications with straight pass-through and a specialized reverse-HTTPS proxy that the AD FS authentication service uses to support cases of certificate authentication (user or device) and other claims-based application access.

In the latter case, the client's secure connection terminates at the edge, and the authentication data is retransmitted securely to AD FS inside the network. This behavior leverages AD FS and allows for conditional access and granular control over how and where the application can be accessed. Many types of applications can be published this way, including apps that support claims, Kerberos-based web apps, Office Forms-Based Access, and apps that use Representational State Transfer, such as OAuth apps.

When publishing custom applications, your developers can leverage Azure Mobile Services to integrate and enhance their apps. Azure Mobile Services provides several capabilities to help developers get going quickly and integrate complex capabilities with little effort, such as linking to data sources, authentication, and configuring push notifications.

Data protection (AD RMS)

Active Directory Rights Management Services (AD RMS) uses encryption to provide another layer of protection for files. Even if a sensitive file (protected with AD RMS) is inadvertently sent by email or stored on a device or medium that is lost or stolen, the file is still protected by AD RMS encryption. Any user who wants to gain access to the file must first authenticate to an AD RMS server to receive the decryption key.

AD RMS provides protection for data both "in transit" and "at rest." The document remains encrypted while being transmitted through email, copied over a network, or even transported physically on media. Traditional in-transit protection technologies, such as Secure Sockets Layer and IP security (IPsec), only protect the information during transmission and sometimes only through certain parts of the network. Because AD RMS protection is contained with and part of the document, wherever the document goes, the protection goes.

While the file is "at rest" on a device, on a server, or even on a portable USB drive, the data remains inaccessible unless the user is authorized to access it. Traditional "at-rest" protection comes from either access control or file or disc encryption. With access control, when a user is authorized to access a file, they can in turn share or retransmit the document without restriction; AD RMS prevents that. With disk-based or file system encryption, including BitLocker Drive Encryption and Encrypting File System, the file is first decrypted on access and again can

usually be shared or transmitted by an authorized user to an unauthorized user or to insecure storage.

Polices such as “do not forward” or “do not print” specify that an authorized user can view a document but only take certain permitted actions. A file can also be set to expire on a certain date, after which previously authorized users can no longer access the file, even if they have made a local copy. AD RMS policies can be configured to require that a user authenticate to an AD RMS server each time a document is opened, or they can be configured to allow cached authentication for a period of time.

When combined with Windows Server 2012 R2 and automatic document classification rules, AD RMS polices can be applied consistently to all important documents within moments of them being placed on a file server. AD RMS also integrates with Microsoft SharePoint, providing automatic protection for document libraries, and with Exchange Server for seamless integration with email content and documents sent via email.

Microsoft has recently released a cloud-based service, Azure RMS, that provides the ability to protect any document type on any platform. Using first-party, “native” applications, such as Office, granular control can be enforced. Microsoft has made a software development kit available to developers so they can build native integration with Azure RMS.

Figure 8 shows typical RMS scenarios.

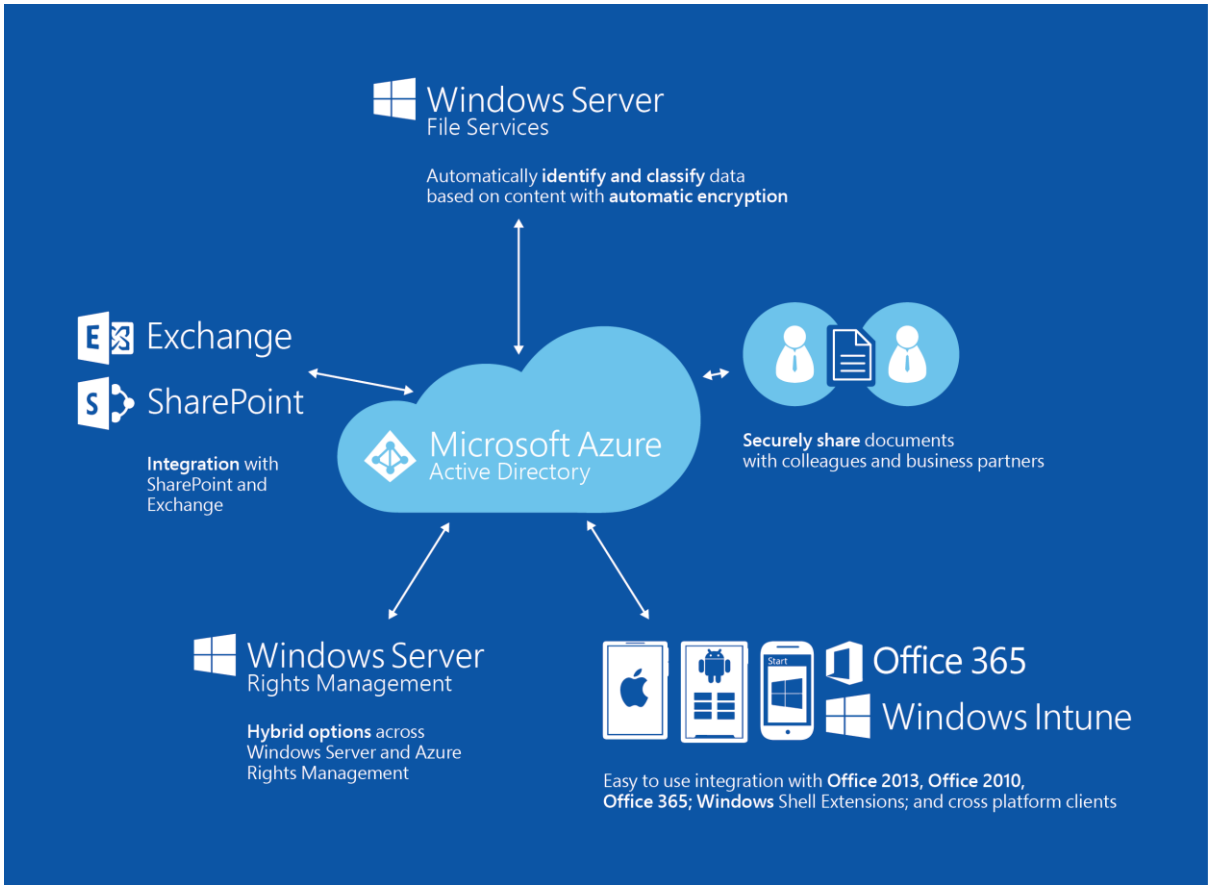

Figure 8. Typical RMS scenarios

Access governance and compliance

In many organizations, it is no longer enough just to control access. Organizations must also be aware of how access is being controlled and be able to report on how access is being granted and used. In other words, you often need to know:

- How data is classified and stored.
- Who has access to that data.
- How or why they were granted access (or who granted it).
- How, when, and where they have used their access.

This rationalized thinking goes beyond just setting up a few access control lists (ACLs). It involves being able to use policy-based tools for provisioning and access control, being able to audit and report, and being able to be both flexible and controlled at the same time.

The common term for this kind of approach is *access governance,* and it's usually considered part of the bigger compliance picture.

Access governance is not a single product, nor is compliance something you can purchase in a retail box, but Microsoft has introduced new software and services to enable you to move to an effective governance model and help you achieve compliance goals. These tools include Microsoft BHOLD Suite Service Pack 1 (SP1) and features in Azure AD, especially Azure AD Premium.

Role-based access control

Microsoft BHOLD Suite SP1 extends the capabilities of FIM by adding role-based access control (RBAC). This lets organizations define user roles and control access to sensitive data and applications in ways that are appropriate for each of those roles.

The BHOLD Suite includes services and tools that simplify the modeling of the role relationships within the organization, map those roles to rights, and verify that the role definitions and associated rights are correctly applied to users. These capabilities are fully integrated with FIM 2010, providing a seamless experience for end users and IT staff alike.

By using the BHOLD Suite, an organization creates several organization units, or *orgunits*. They are similar in hierarchy to OUs in LDAP or AD DS, except that a user can be a member of multiple orgunits. This is because orgunits reflect job roles.

For example, a company may have a structure similar to that shown in Figure 9. In this case, a sales representative may have roles related to being in the West region but also roles related to being in Retail or Corporate Sales.

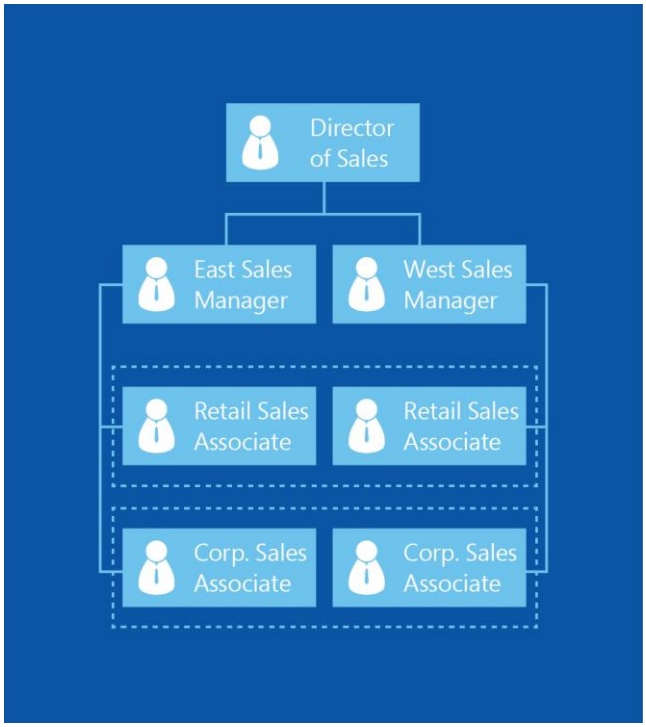

Figure 9. A typical corporate structure

What sets RBAC apart from typical discretionary access solutions (those like NTFS permissions that are based on discretionary ACLs) is that permissions for resources are not assigned to users or even to groups but are based on the roles a user holds.

The BHOLD Suite contains the tools needed to plan and implement an RBAC structure with Windows Server and FIM.

Segregation of duties

Another important concept in security and governance is that duties should be divided, or *segregated,* and not assigned to one person only. For example, the person who performs an auditable function, such as backing up confidential information to removable media, should not be the same person who can clear the audit logs of that event.

Separation of duties (SoD) is both a security concept and a business concept. A common business example is that the person who requests a payment is not the same person who can authorize that payment. It is up to the IT department to implement technology solutions that can enforce the business concepts of SoD as well as the technical and audit rules.

The BHOLD Suite implements SoD by letting you define incompatible permissions. When these permissions are defined, the BHOLD Suite enforces SoD by preventing the creation of roles that are linked to incompatible permissions, whether they are linked directly or through

inheritance. The BHOLD Suite prevents users from being assigned multiple roles that, when combined, would grant incompatible permissions.

Workflow approvals

Using FIM, you can define workflows to require more than one level of approval when users request access to resources. FIM routes the requests through the approval process as defined and notifies the user of the outcome.

Attestation

Sometimes, a company will need to "attest" that individual users have been given access in accordance with policies. The BHOLD Suite provides tools that can help verify that individual users have the appropriate permissions for their business tasks.

An administrator can use the BHOLD Attestation module portal to manage the attestation process. The process uses campaigns in which campaign stewards verify that users have appropriate access to BHOLD Suite–managed applications and correct permissions within those applications. Typically, the steward for a campaign will be a manager who is responsible for users in one or more orgunits, and who will attest that the correct access rights are applied.

A campaign can be created to occur once or on a recurring basis.

Cloud-based governance with Azure AD

The BHOLD Suite and FIM can bring a formal methodology to identity governance, especially for on-premises applications, but because your users and applications are moving to the cloud, your compliance must, as well.

Azure AD Premium, built on top of the free offering of Azure AD, provides a robust set of capabilities to empower enterprises that have more demanding needs on identity and access management (Figure 10).

In its first milestone, Azure AD Premium offers:

- **User self-service password reset.** For your end users, the Premium offering of Azure AD will provide self-service password reset capabilities for cloud applications.
- **Group management.** Azure AD Premium offers group-based access management to SaaS applications.
- **Company branding.** To make the end user experience even better, the **Access Panel** page can now support the addition of company logos and color schemes.

- **Security reports.** Use detailed machine learning–based reports showing sign-in activity, anomalies, and potential threat areas.

With this first milestone release, security reporting can offer meaningful insights. Reporting on anomalies such as who signed in from unknown sources; successful logins after multiple failures; or the "impossible travel" scenario, where someone logs in from multiple geographies in too short a timeframe.

Azure AD Premium will continue to grow and embrace new identity and access management requirements of the cloud era.

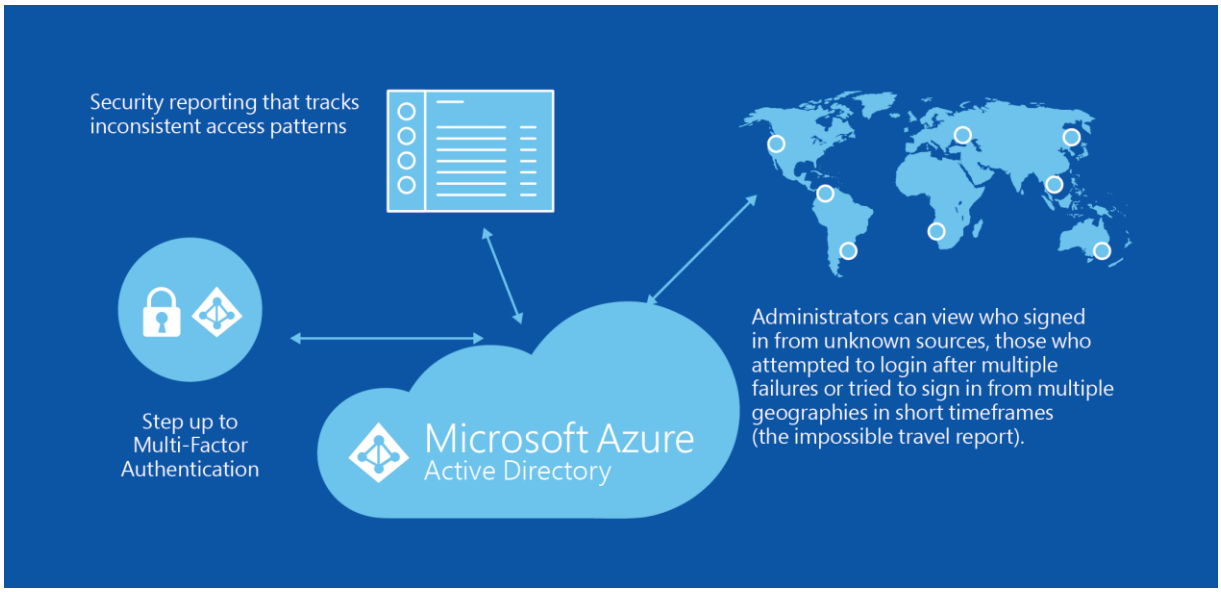

Figure 10. Azure AD Premium offerings

Workload example: SharePoint with conditional access, MFA

Contoso has implemented SharePoint for employee collaboration, document management, and workflow. SharePoint now contains a great deal of confidential information. Some of the files and data are subject to legislation and regulations.

Contoso management is concerned that access to this information be properly controlled. Users, especially mobile employees in sales, have been clear that they require access to the information at any time and from any place.

Contoso has classified the files, applications, and data into low, medium, and high risk (Figure 11). By implementing Azure AD MFA, Contoso has implemented the following elements:

- Low-risk items can be accessed by using a user name and password from any device on any network.
- Medium-risk items can be accessed only on domain-joined computers or registered mobile devices.
- High-risk items can be accessed only on domain-joined computers or registered mobile devices and require MFA.

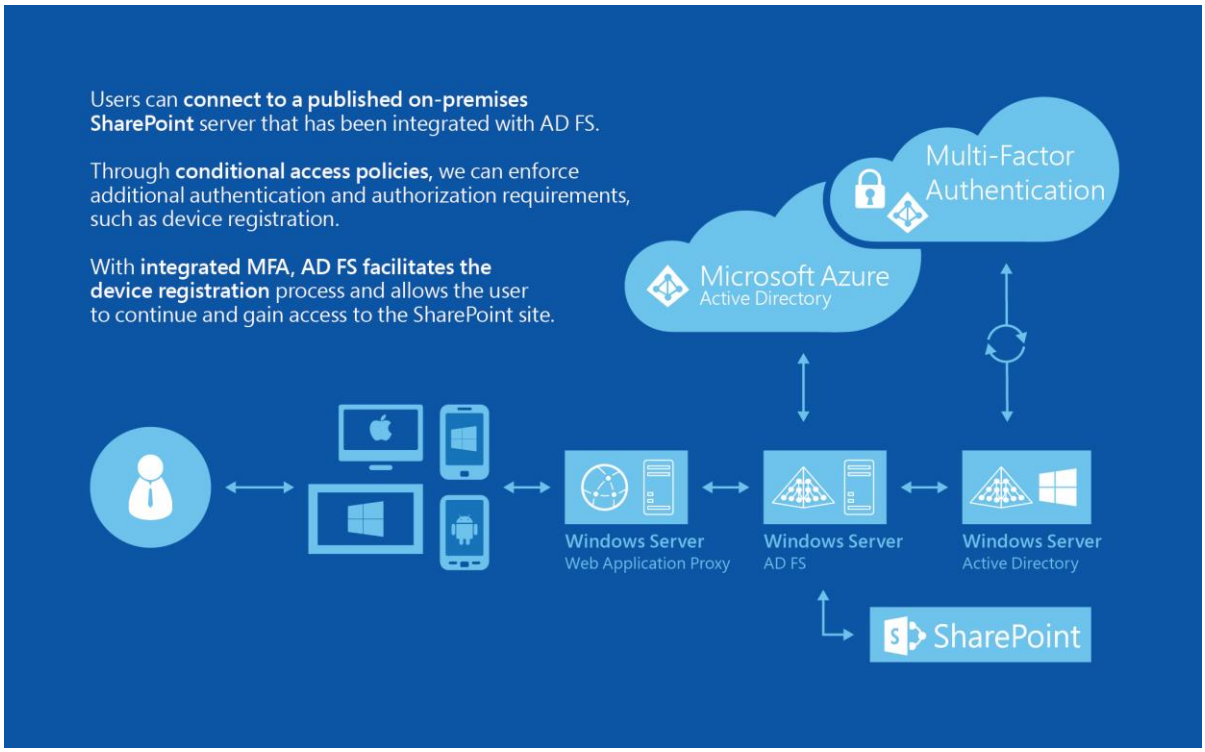

Figure 11. Contoso's SharePoint configuration

Conclusion

Across the people-centric IT scenarios and solutions, we think about delivering on the needs of users and IT in three distinct ways.

Enable users

Enabling users is about ensuring that users can work on the device of their choice and access resources they need to get their jobs done. Key elements include registration and enrolment for devices, self-service through the company portal, automatic virtual private network connections, SSO, and synchronization of data with Work Folders.

Hybrid Identity

You need to manage the complexity of existing platforms and add new capabilities to deliver cloud-based services to organizationally managed devices and user-provided devices, regardless of where the services are delivered and consumed from. Microsoft can help you deliver this through a strong common identity that allows for unified management and single-credential access to resources on-premises, in the cloud, and federated with partners and SaaS providers.

Protect your data

Users want to be able to access their information on their own devices, but the company must ensure that corporate compliance policies are followed. Companies can choose to centralize corporate information for compliance and data protection, and then enable data sync to devices in a controlled way, along with creating policy-based access control for applications and data, taking into account the user's identity, whether the user's device is "known" (registered), and also the location—whether they are internal or external to the corporate environment.

For more information

More information about technologies and products mentioned in this paper is available from the Microsoft website.

Related products

- Windows Server 2012 R2
- Microsoft System Center 2012 R2 Configuration Manager
- Windows Intune
- Azure Active Directory
- Forefront Identity Manager

Related solutions

- User and Device Management
- Access and Information Protection

Technical resources

- Access and Information Protection
- Active Directory in Windows Server 2012 R2
- Active Directory Federation Services
- Azure Active Directory: Scenarios and Solutions
- How to Authenticate Web Users with Azure Active Directory Access Control

Azure AD resources

- Azure Active Directory
- Active Directory Team Blog
- Active Directory Authentication Library 1.0 for .NET
- Azure Application Gallery for cloud apps
- Active Directory Considerations in Azure Virtual Machines and Virtual Networks
- Setting up Azure Active Directory ACS to provide identities to Azure Pack
- Federated Identities to Azure Pack through AD FS
- Azure Active Directory service page

- Azure Multi-Factor Authentication service page
- Azure Active Directory documentation page